S. HRG. 104–729

THE AVAILABILITY OF BOMB-MAKING INFORMATION ON THE INTERNET

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED FOURTH CONGRESS

FIRST SESSION

ON

EXAMINING THE IMPLICATIONS OF THE AVAILABILITY OF BOMB-MAKING INFORMATION ON THE INTERNET

MAY 11, 1995

Serial No. J–104–25

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1996

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-053965-X

S. HRG. 104–729

THE AVAILABILITY OF BOMB-MAKING INFORMATION ON THE INTERNET

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED FOURTH CONGRESS

FIRST SESSION

ON

EXAMINING THE IMPLICATIONS OF THE AVAILABILITY OF BOMB-MAKING INFORMATION ON THE INTERNET

MAY 11, 1995

Serial No. J–104–25

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1996

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-053965-X

STROM THUI
ALAN K. SIM
CHARLES E.
ARLEN SPEC
HANK BROW
FRED THOMI
JON KYL, Ari
MIKE DEWINI
SPENCER AB

KF 4772 .A2 A93 1997
United States. Congress.
Senate. Committee on the
The availability of bomb-
making information on the

ietts

DATE	ISSUED TO

TERRC

)N

FRED THOMP
SPENCER ABI
STROM THUR

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

CHRONOLOGICAL LIST OF WITNESSES

ALPHABETICAL LIST AND MATERIALS SUBMITTED

APPENDIX

QUESTIONS AND ANSWERS

Page

ADDITIONAL SUBMISSIONS FOR THE RECORD

THE AVAILABILITY OF BOMB-MAKING INFORMATION ON THE INTERNET

THURSDAY, MAY 11, 1995

U.S. SENATE,
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY,
AND GOVERNMENT INFORMATION,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:33 a.m., in room 226, Dirksen Senate Office Building, Hon. Arlen Specter (chairman of the subcommittee) presiding.

Also present: Senators Kohl, Leahy, and Feinstein.

OPENING STATEMENT OF ARLEN SPECTER, A U.S. SENATOR FROM THE STATE OF PENNSYLVANIA

Senator SPECTER. I don't like to use the gavel, but I think we need it this morning so we can proceed with this hearing of the Judiciary Subcommittee on Terrorism, Technology, and Government Information.

This is the third hearing in a schedule of five hearings where we are looking into the problems of terrorism in the United States. The first hearing had been scheduled long in advance of the Oklahoma City bombing to take up the contents of legislation which had been suggested by the administration.

That hearing was then held on April 26. Then, on May 4, last Thursday, we had the second hearing, taking up considerations from the American Civil Liberties Union, the American Jewish Congress, and the African American League.

Today, we are moving ahead on the hearing on the so-called mayhem manuals. Next week, the subcommittee had scheduled a hearing on Waco and Ruby Ridge, which may be held by the full committee. Our initial hearing, which had been scheduled by the subcommittee, was held by the full committee so that more Senators could participate—and right now, we are trying to make a determination as to precisely how the hearing will be held on Waco and Ruby Ridge. It is my view that it is important to move ahead with some promptness on that hearing because there is a very substantial amount of concern in America about what happened at Waco.

That is a matter for which I have been pushing for a hearing, since the summer of 1993. I have also sought hearings on what happened at Ruby Ridge, ID. I think it is no coincidence that the Oklahoma City bombing was 2 years to the day, April 19, after the incident at Waco.

I think it is important that the Senate should not stand aside and not act when there is so much public concern, lest our inaction produce something else. I don't want to make any self-fulfilling prophecies, but I do think it is important to move ahead.

My suggestion is embodied in a sense-of-the-Senate resolution, which is now pending in the Senate, to move ahead with that hearing on or before June 30, 1995.

The subcommittee will have a fifth hearing on May 25 on the subject of the militia movement, which will conclude the hearings which we have outlined to be held in advance of Labor Day.

Today's hearing is on the so-called mayhem manuals. I think this is a very, very important hearing because it poses on the cutting edge the issue of freedom of speech versus public protection.

Shortly after the Oklahoma City bombing, a message was transmitted on the Internet which said:

> Are you interested in receiving information detailing the components and materials needed to construct a bomb identical to the one used in Oklahoma? The information specifically details the construction, deployment, and detonation of high-powered explosives. It also includes complete details of the bomb used in Oklahoma City, and how it was used and how it could have been better. The information will be provided to anyone who properly requests it and is provided solely for informative purposes.

The last sentence obviously was designed to add a disclaimer.

In the Internet, we now have an international, cooperative computer network of more than 28,000 computer networks in 60 countries, which links many types of users such as governments, schools, libraries, corporations, individuals, and others. So, the issue of dissemination is now just enormous, and really overwhelming.

Available on the Internet is a voluminous manual entitled, The Big Book of Mischief," covering some 93 pages. There are instructions on how to make a bomb with ammonium nitrate, how to make what they call an easy Molotov cocktail, which can be constructed by a 10-year-old, and how to manufacture book bombs. The concerns and the problems are self-evident.

Against that, we have the longstanding first amendment guarantees in the United States, exemplified by the Supreme Court decision in *Brandenburg* v. *Ohio,* which says:

> The constitutional guarantees of free speech and free press do not permit a State to forbid or prescribe advocacy of the use of force, of law violation, except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or product such action.

There has been a recorded case by the U.S. district court in Wisconsin which involves a prior restraint on the dissemination of a book which tells you how to make a hydrogen bomb. That particular decision implicates the Atomic Energy Act, so it is a little different, and we have with us today, Prof. Frank Tuerkheimer, who represented the Government in that case.

In the intervening days since the Oklahoma City bombing, I have had discussions with many lay people and many lawyers on the unique kinds of problems which we face, here. The response of so many people is: How can we permit these mayhem manuals from being distributed, especially over the Internet?

You have to judge that against a long history of constitutional rights. The strength of our democracy, the strength of our Republic,

I think, is rooted very basically in our freedom of speech and freedom of press, which we want to protect.

That is the sort of an intersectional conflict which we are going to be looking at here today.

We have a very distinguished group of witnesses and I welcome, at this time, Rabbi Marvin Hier, dean of the Simon Wiesenthal Center from Los Angeles; Mr. Robert S. Litt, Deputy Assistant Attorney General; Mr. William Burrington, assistant general counsel and director of government affairs, for America Online; Mr. Jerry Berman, executive director, Center for Democracy and Technology; and as I said, Prof. Frank Tuerkheimer.

I have a commitment on the Intelligence Committee, which will require my excusing myself for a few moments, at about 10:15, but up until that point, and shortly after that point, I will be here for the entire hearing.

We welcome you, Rabbi Hier, and look forward to your testimony. All of your statements will be made a part of the record, as is our custom, and as is also our custom, we ask that you summarize those, leaving the maximum amount of time for questions and answers.

[The prepared statement of Senator Specter follows:]

PREPARED STATEMENT OF SENATOR ARLEN SPECTER

I welcome everyone to this hearing of the Subcommittee on Terrorism, Technology and Government Information on "Mayhem Manuals on the Internet."

This is the third in a series of hearings regarding terrorism held since the bombing of the Federal Building in Oklahoma City. The first hearing, held by the full Judiciary Committee, focused on the nature and extent of the terrorist threat in the United States from both transnational and domestic terrorists. The second hearing, held last week, focused on pending counterterrorism legislation, with a special emphasis on civil liberties concerns raised by these bills.

This hearing focuses on the use of the Internet by a variety of groups and individuals to propagate "mayhem manuals," which, as they name suggests, are guides to assist people in committing acts of violence.

The Internet is an international, cooperative computer network composed of over 28,000 computer networks in 60 countries. The Internet links thousands of users of all types: governments, schools, libraries, corporations, non-profits, individuals, virtually all users of computers can gain access to the Internet. No one controls the Internet. It is a cooperative group of computer networks. It is the most democratic means of communication today. Without going through an intermediary, a person on the Internet can communicate with all other users.

The Internet represents a revolutionary form of mass communication. No longer does someone need to write a book that others must purchase or speak over the radio or television that others can turn off in order to reach mass audiences. No longer does a person who wishes to communicate have to rely on the vagaries of the market, or an editor, or time constraints. On the Internet, people from all over the world can communicate directly with each other.

Among those who communicate on the Internet are purveyors of hate and violence. Among the full text offerings on the Internet are detailed instruction books describing how to manufacture a bomb. The most widely known manual is the "Big Book of Mischief." This 93-page document details explosives formulas, how to purchase explosives and propellants, and how to use them. For example, on page 37, the anonymous author describes how to make a Molotov cocktail from household products. Anyone with access to the Internet can obtain this recipe for disaster, even a 10-year-old child who can find a glass container and some gasoline. I am troubled that we may one day fondly recall the days of prank phone calls once these mayhem manuals permeate our schools. Already, one inquiry on how to construct a bomb reportedly was made by a 13-year-old. I doubt that this inquiry was the result of a school project.

There are also electronic mail discussion groups where information on bomb making can be traded anonymously. One disgusting example is this anonymous message posted on an Internet electronic bulletin board shortly after the Oklahoma City

bombing: "Are you interested in receiving information detailing the components and materials needed to construct a bomb identical to the one used in Oklahoma. The information specifically details the construction, deployment, and detonation of high powered explosives. It also includes complete details of the bomb used in Oklahoma City, and how it was used and how it could have been better." The individual who posted this message, who cowers in anonymity, deserves condemnation for using the Internet to suggest how the Oklahoma City bombing "could have been better." This is just one of many other examples. The media have reported that a variety of hate groups and militias use the Internet to gain adherents, organize, and rally support.

Among the issues before us are the extent of such usage of the Internet and whether anything can or should be done to curb it.

There are serious questions about whether it is technologically feasible to restrict access to the Internet or to censor certain messages. If that is not feasible, then the government would only be able to act after the fact to punish those who misuse the Internet.

Even if the technological issues can be resolved, there remain significant First Amendment concerns. The governing standard under the First Amendment was established in *Brandenburg* v. *Ohio,* decided in 1969. The Supreme Court held that speech could not be punished unless it was an incitement to imminent lawless action. Cases upholding restrictions on speech are extremely rare. Perhaps the most famous is the case involving The Progressive magazine, which was enjoined from publishing an article that detailed how to build a hydrogen bomb. We have with us today the United States Attorney who handled that case for the government, Frank Tuerkheimer, now a professor of law at the University of Wisconsin.

Some scholars, perhaps most notably former Judge Robert Bork, however, have argued that the First Amendment's protections do not extend so far as to protect speech outside the political context. While that may be too narrow a reading of the First Amendment, we should not forget the warning of Justice Robert Jackson that the Bill of Rights must never be converted into "a suicide pact."

With these issues before us, I would like to welcome our witnesses to this hearing. We will hear from Deputy Assistant Attorney General Robert S. Litt of the Criminal Division of the Department of Justice; Rabbi Marvin Hier of the Simon Wiesenthal Center in Los Angeles, which tracks the use of the Internet by groups and individuals that distribute mayhem manuals and similar materials over the Internet; Professor Frank Tuerkheimer of the University of Wisconsin Law School; Mr. William W. Burrington, assistant general counsel of America Online, who is testifying on behalf of the Interactive Services Association; and Mr. Jerry Berman of the Center for Democracy and Technology. We welcome all the witnesses and thank them for coming.

Senator SPECTER. I yield, first, however, to my distinguished ranking member, Senator KOHL.

STATEMENT OF HON. HERB KOHL, A U.S. SENATOR FROM THE STATE OF WISCONSIN

Senator KOHL. Thank you very much, Mr. Chairman.

Mr. Chairman, most Americans don't know what is out there on the Internet. If they did, they would be shocked. While the vast majority of information is useful and valuable, the information superhighway has dark back alleys.

As you have pointed out, anyone proficient enough to navigate it can obtain things like bomb recipes, hate literature, terrorist manuals, lewd photographs, or they can participate in adult chatrooms, and some of the most adroit navigators, unfortunately, are children.

For example, just days before the explosion in Oklahoma, a 12-year-old Missouri boy downloaded a recipe off the Internet and constructed a crude napalm bomb. All it took was gunpowder, gasoline, and foam chips. Fortunately, his father found the bomb before it detonated and turned it in to the local police.

Indeed, in just an hour and a half of surfing the Internet, my staff and the Congressional Research Service uncovered the follow-

ing materials: "How to Build an Atomic Bomb," "The Terrorist Handbook," "How to Pick a Lock," "The World Sex Guide to Prostitution," and many, many sex bulletin boards. Under no circumstances should these materials be made available to our children.

You parents watching this hearing need to know that your children can get hold of these materials, and we need to work together to find a better way to stop it.

Still, while there are many items on the Internet that we would personally want to restrict, we must remember our obligations under the first amendment. The Government should not be in the business of telling people what they can and cannot think, but the Government can certainly act to prevent people from endangering public safety.

So the question we are facing is this: What kind of action needs to be taken, and by whom?

Well, first, parents should be notified every time their child opens an online account. This is easy because opening an account usually involves the use of a credit card.

Second, every parent should easily be able to block their child's access to certain areas of the Internet. If we have the technology to get children on the Internet, we should have the technology to get them off it.

Third, online companies should look to the video game industry, where industry-wide cooperation to restrict access to minors has forestalled Government intervention.

In other words, the industry should act now, or Congress will do it for you.

Finally, aside from industry or Government efforts, we must challenge parents to take responsibility to monitor their children's activities. The Internet is not a full-time babysitter. It is a 21st century playground, and as with most of today's playgrounds, you should watch your kids or they will get into trouble.

We must also challenge those who publish on the Internet to think about the impact of their words and contemplate the consequences of their actions on the information superhighway. Hopefully, last month's bombing has started this process.

Mr. Chairman, just a word of caution. We should not overreact to this problem. We must try our hardest to clean up the back alleys of the superhighway, but we must also be sure that our zest for sweeping them clear does not spill over to harm innovative activities.

We need to keep in mind that many of these mayhem manuals are easier to find in libraries or in bookstores than on the Internet. "The Anarchist Cookbook" is readily available at many neighborhood bookstores, and basic explosive recipes can be found in many chemistry books. If someone wants to find this information, in a free society, he or she can locate it.

Finally, I am pleased to see that my friend, Frank Tuerkheimer from the University of Wisconsin is testifying today. A former U.S. attorney, Frank was a prosecutor in the famous *United States* v. *Progressive* case. No one knows better than Frank how hard it is to balance free speech and national security.

We look forward to hearing his perspective, as well as all the members of our panel, and we thank the chairman for today's hearing.

[The prepared statement of Senator Kohl follows:]

PREPARED STATEMENT OF SENATOR HERB KOHL

Mr. Chairman, most Americans don't know what is out there on the Internet. And if they did they would be shocked. While the vast majority of information is useful and valuable, the information superhighway has dark back alleys. Anyone proficient enough to navigate it can obtain bomb recipes, hate literature, terrorist manuals, lewd photographs or participate in adult chatrooms. And frighteningly, some of the most adroit navigators are children.

For example, just days before the explosion in Oklahoma, a 12-year-old Missouri boy downloaded a recipe off the Internet and constructed a crude napalm bomb. All it took was gunpowder, gasoline and foam chips. Fortunately, his father found the bomb before it detonated and turned it in to the local police.

Indeed, in just an hour-and-a-half of surfing the Internet, my staff and the Congressional Research Service uncovered the following materials: "How to Build an Atomic Bomb," "The Terrorist Handbook," "How to Pick a Lock," "The World Sex Guide to Prostitution" and many, many sex bulletin boards. Under no circumstances should this be available to our children. Period.

You parents watching this hearing need to know that your children can get hold of these materials. And we need to work together to find a better way to stop it.

Still, while there are many items on the Internet that we would personally want restricted, we must remember our obligations under the first amendment. The Government should not be in the business of telling people what they can and cannot think. But the Government can certainly act to prevent people from endangering public safety.

So the question is this: What kind of action needs to be taken and by whom?

First, parents should be notified every time their child opens an on-line account. This is easy because opening an account usually involves the use of a credit card.

Second, every parent should easily be able to block their child's access to certain areas of the Internet. If we have the technology to get children on the Internet, we should have the technology to get them off it.

Third, online companies should look to the video game industry, where industry-wide cooperation to restrict access to minors has forestalled Government intervention.

In other words, the industry acts now or Congress will do it for you.

Finally, aside from industry or Government efforts, we must challenge parents to take responsibility to monitor their children's activities. The Internet is not a full-time baby-sitter. It is a 21st century playground and, as with most of today's playgrounds, you should watch your kids or they can get into trouble.

We must also challenge those who publish on the Internet to think about the impact of their words—and contemplate the consequences of their actions on the information superhighway. Hopefully last month's bombing has started this process.

Mr. Chairman, a word of caution. We should not overreact to this problem. We need to try our hardest to clean up the back alleys of the superhighway. But we must also be sure that our zest for sweeping them clean does not spill over to harm innovative activities.

We need to keep in mind that many of these mayhem manuals are easier to find in libraries or bookstores than on the Internet. "The Anarchist Cookbook" is readily available at many neighborhood bookstores, and basic explosive recipes can be found in many chemistry books. If someone wants to find this information, in a free society he or she can locate it.

Finally, I am pleased to see that my friend, Frank Tuerkheimer from the University of Wisconsin is testifying today. A former U.S. attorney, Frank was a prosecutor in the famous *U.S.* v. *Progressive* case. No one knows better than he how hard it is to balance free speech and national security. We look forward to hearing his perspective, and I thank the chairman for today's hearing.

Senator SPECTER. Thank you very much, Senator Kohl. Senator Leahy.

STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Thank you, Mr. Chairman. I also applaud you for having this hearing and the series of hearings that you have had. What you and Senator Kohl have done here, I think, is extremely important.

I believe, as I know you do, that when you have tragic events like the bombing in Oklahoma City, it requires us all to think about what we can do to make this a safer and a better world, and I hope this hearing will help.

I also hope that in these difficult days, we do not lose sight of those values that make this the strongest and most vibrant democracy in the world. We are an open and free society and we have to remain faithful to the first amendment of the U.S. Constitution.

Some complain that the Internet is too free, it is too open to expression, it is too communicating. Well, I understand that frustration. I understand that fear. I do share their concern that young people not be corrupted, and also as a parent, I want to know that parents can control how they raise and educate their children.

I abhor hateful speech. I abhor the rantings of those who wrongly believe that every action of the Federal Government, and even events in which the Federal Government had no part, are somehow a secret plan to restrict individual rights in this country. But, I also disagree with those who would opt for repression.

We have a lot of people who say things that are so stupid and so beyond the pale that I would hope that in a free society, that that itself would stop it.

I am concerned when I see people send out letters, fundraising letters, that in effect declare the President of the United States has committed murder. Obviously, if they feel that way, why aren't they seeking indictments? I mean, this is an indictable offense. It certainly would be an impeachable offense. But, it is also a stupid assertion; except that it makes money for some people.

I abhor those who stand up and talk about using the picture of the President of the United States for target practice. I mean—my God—this is a country that has seen itself so devastated by Presidential assassinations. Just since I have been old enough to vote, I have seen the assassination of one President, the wounding of another, and an attempt on a third.

These are not things that we should treat so lightly. But we are a free society, we do have the first amendment, and before we head down a road that leads to censorship, we ought to think about it.

The same first amendment that protects each of us and our right to think and speak as we choose, protects these others, as well.

The rule of this free society has long been that it is harmful and dangerous conduct—not speech—that justifies adverse legal consequences, so I caution careful deliberation and consideration of what our new technology can bring us before we ask the Government to act to restrict it and limit its uses and usefulness. The better approach might be to seek to engage those estranged from society in conversation and dialog, rather than to exclude them and simultaneously fuel their paranoia.

So, Mr. Chairman, I would put into the record my whole statement, if I might, and I would also note that we have very recently

received a letter from the Department of Justice analyzing the obscenity restrictions in the telecommunications bill. The Department points out that not only would they not work, but they would actually frustrate the Department's aggressive enforcement of existing obscenity and child pornography laws. The Department asks for further deliberation and study on this, which is what I have called for in S. 714, a bill I introduced along with Senators Kohl and Kerrey, in that regard.

I would ask that my whole statement be made part of the record.

[The prepared statement of Senator Leahy follows:]

PREPARED STATEMENT OF SENATOR PATRICK J. LEAHY

Tragic events, like the bombing in Oklahoma City, require us all to examine what more we can do to make this a better and a safer world. This hearing is one in a series held by this Subcommittee and complements those held by the Judiciary Committee and other committees of Congress in this regard.

In these difficult days, I caution that we not lose sight of those values that make this the strongest, most vibrant democracy in the world. We are an open and free society and we should remain faithful to the First Amendment of the United States Constitution.

Some complain that the Internet is too free, too open, too expressive and too communicating. I understand their frustration and their fear. I share the concern that young people not be corrupted and that parents be able to raise and educate their children. I abhor both hateful speech and the rantings of those who wrongly believe that every action of the Federal Government and even events in which the Government played no part are part of some secret plan to restrict individual rights in this country. But I also disagree with those who would opt for repression.

Before we head down a road that leads to censorship, we must think long and hard about its consequences. The same First Amendment that protects each of us and our right to think and speak as we choose, protects these others, as well. The rule of this free society has long been that it is harmful and dangerous conduct, not speech, that justify adverse legal consequences.

I caution careful deliberation and consideration of what our new technology can bring us before we ask the Government to act to restrict it and limit its uses and usefulness. Might the better approach be to seek to engage those estranged from society in conversation and dialogue, rather than to exclude them and simultaneously fuel their paranoia?

In this area, we need to be sure we are not vainly striking out at a medium of communication because we are frustrated by not being able to identify the person or group responsible for separate, criminal action.

At an earlier hearing, Director Freeh of the FBI acknowledged that instructional materials on bomb making are otherwise available in paper formats. Thus, I submit that little is to be gained in the way of safety by banning such communications over electronic media. Those who want to find it can, and likely will.

Further, we should consider whether legitimate law enforcement activities would be hindered by further isolating those who espouse extremist views. The FBI Guidelines have long contemplated investigation when "statements advocate criminal activity or indicate an apparent intent to engage in crime, particularly crimes of violence" and authorized domestic terrorism investigations when facts and circumstances" reasonably indicate that two or more persons are engaged in an enterprise for the purpose of furthering political or social goals wholly or in part through activities that involve force or violence and a violation of the criminal laws of the United States." Such investigations can make use of public records and sources of information and, when authorized, stored wire and electronic communications.

On the similarly charged subject of obscenity on computer networks, some have been quick to propose restrictions. While well motivated, they have included restrictions in the telecommunications bill that the Senate is about to consider, S.652, that do not withstand scrutiny. On that subject, I likewise cautioned thoughtfulness and called for study of possible technological means and other alternatives to help parents and others better control access to computer network information.

I recently received a letter from the Department of Justice analyzing the obscenity restrictions in the telecommunications bill. The Department concludes that they will not work but will, instead, frustrate the Department's aggressive enforcement of existing obscenity and child pornography laws, at the same time that they threaten important First Amendment and privacy rights.

The Department recommended deliberation and further study in that important area, which is exactly what I called for in S. 714, the bill I introduced on this subject earlier this session with Senators Kohl and Kerrey.

Likewise in this area of violent speech, we should not rush to renounce our fundamental commitment to First Amendment values. While maintaining freedom of speech is not without risk, we will have already lost when we adopt censorship and repression. Speech with which we disagree is best met by more speech, not less; by debate, not denial; and by sunshine, not darkness.

I look forward to hearing from our distinguished panel here today and to continuing this important conversation, which exemplifies our resilient and open democracy.

Senator SPECTER. It will be made part of the record, and my statement, as well, and Senator Kohl's.

Rabbi Hier, the floor is yours.

STATEMENT OF RABBI MARVIN HIER, DEAN, SIMON WIESENTHAL CENTER, LOS ANGELES, CA

Rabbi HIER. Mr. Chairman, Senators, in the interest of time, I would like to enter my entire statement, but I would like to begin on page 2.

Let me begin by reading a recent posting from the Internet:

We need to begin the revolution now, without delay. Hopefully you all know the revolution of which I speak. The revolution to cleanse our grand nation of the undesirables (niggers, beans, jews, the like) and return the white man to his rightful place atop America. The Oklahoma City bombing was a government setup to discredit the militias and whi[t]e activists. We need to begin our fight to eradicate the Federal Government, dominated by Jews since the 30's, beholden to the NAACP and alike organizations. If we do not act soon, we will let America slip into the doldrums of racial equality. I am by no means crazy, just realistic. The white man, superior to all, as I hope you realize, needs to assert his power. I will be leading my mil[i]tia in southern Califronia [California] against targets in the southwest. Join me to free America!

Mr. Chairman, in a sense, this statement—posted on May 7, 1995, by a self-proclaimed racist militiaman summarizes why we are here today. First, permit me a brief comment on the militias, themselves.

Are they a threat to America? The only conclusion you can reach after reading manuals like those distributed by the Militia of Montana—the entire manual, I have here—is yes. They intend to be a threat to this country.

When a man stands before you and says that he hates everything that you stand for and wants to kill you and has a gun in his hand, he is certainly a threat.

These groups encourage their followers to prepare for self-prophesied doomsday scenario and give the specifics of how to hasten it. Assaults on the most vulnerable targets, such as commercial and industrial enterprises, police stations, government property, mass communication media, ships, trains, planes; liberation of prisoners and creation of riots in penal institutions; kidnaping of renowned artists and sports figures; acts of sabotage, particularly on firms and properties not owned by Americans.

The manual accuses the Federal Government of controlling education and the press and regularly using the IRS to spy. Even before Waco, the manual details an escalating series of alerts which could lead to the inevitable violent confrontation with Federal law enforcement officers.

Mr. Chairman, today it is the militias. Tomorrow, it can be their own courts and senates and their own commander in chief. America cannot and should not tolerate private armies, they are a recipe for potential anarchy, violence, and civil disorder.

More specifically, Mr. Chairman, on the issue of the Internet. The Wiesenthal Center has located, both prior to and since the Oklahoma massacre, numerous recipes for building bombs. Information once in a few counterculture bookstores is now daily promoted into millions of American homes.

Under our system of laws and freedoms, we are unable to stop the flow of such dangerous information to people bent on destruction. But, America can and must prohibit the over-the-counter sale of large quantities of chemicals like ammonium nitrate and other explosives or toxic substances to people who have no legitimate use for them. A licensing procedure would at least make it more difficult for potential terrorists to anonymously carry out their plans.

Further, we believe that in view of the bombings at the World Trade Center and Oklahoma City, that the consideration of controls on sales of such items be considered by the Congress with all deliberate speed and not the 1-year period suggested in section 103 of President Clinton's proposed antiterrorism legislation.

Mr. Chairman, the threat I quoted in my opening remarks is indicative of the increasing high-technology traffic by America's hate groups. Today, the Wiesenthal Center has logged over 50 such groups utilizing various elements of cyberspace—from electronic bulletin boards to sophisticated Web sites on the Internet.

The reasons for this troubling trend are quite clear. Cyberspace offers direct, instantaneous, cheap, mainstream communications in the marketplace of ideas. Further, young people—a target group for racists—are especially drawn to this cutting edge of technology.

Cyberspace has suddenly empowered marginal local groups, be they overt white supremacists or militias with racist ties, like the Northern Regional Militia of Michigan, these groups market nationally inflammatory videos and computerized files which fuel a conspiratorial, rabidly antigovernment, and, often, violent world view.

The information superhighway also empowers local militia and hate group members with a sense that they are a part of an increasingly powerful nationwide movement. In addition to the obvious mainstream marketing capabilities, available technology also permits, when desired, anonymity when launching hate attacks on the Internet.

So, what can or should be done with a decentralized network of more than 50,000 interconnected networks flowing to some 30 million computers?

First, if nothing else, we need to give law enforcement the opportunity and capability to monitor hate and violence-oriented posting in cyberspace. We believe authorities will be unable to effectively keep tabs on trends and potentially illegal activity if they cannot do what amounts to the equivalent of clipping a newspaper article by downloading a file on the Internet.

We are not advocating an attack on cherished first amendment freedoms. However, we do believe that law enforcement should be

free to investigate clearly expressed intentions to commit violence, such as was expressed in the Internet posting that I quoted.

Second, Mr. Chairman, we also need the attention and leadership of technology providers to help America marginalize the hate-mongers. As you know, online and Internet access providers sell a service to the public, and we are happy to report that, in some cases, these providers are already taking a pro-active stand to bar their services from such hate-mongers.

Third, in evaluating any potential course of action, we should evaluate the particular format and function of the use of the high technology superhighway to see what limits, if any, should be applied. So, for example, we need to keep in mind that the obscene or threatening phone caller has neither the privacy nor his speech protected when he threatens a member of the community via the telephone.

Senator SPECTER. Rabbi Hier, could you summarize, in conclusion, please?

Rabbi HIER. Yes, I will just finish, here.

Why are those protections afforded if he launches the same attack via the Internet?

I will just end, there.

[The prepared statement of Rabbi Hier follows:]

PREPARED STATEMENT OF RABBI MARVIN HIER

Mr. Chairman: My name is Rabbi Marvin Hier. I am the Dean and Founder of the Simon Wiesenthal Center and of the Museum of Tolerance, an international Jewish human rights agency that monitors and confronts hate groups and terrorist groups in the United States and abroad.

On the International scene, during the Gulf War, the Center published "The Poison Gas Connection," which identified more than 400 Western companies that were supplying Sadam Hussein with potent chemicals and gasses in the months preceding the Gulf War.

The Center was also amongst the first to warn the United States that the leaders of Hamas and Islamic Jihad were using the United States as a base of operations for fundraising and public information and that leading members of Hamas and Islamic Jihad were coming to the U.S. to participate in conferences in the mid' 80s.

More recently, in 1993, the Center placed someone inside the neo-Nazi movement in Germany for seven months where he closely observed the workings of more that 30 neo-Nazi groups.

On the domestic front, the Center, through its Museum of Tolerance, regularly monitors more than 240 hate groups, from neo-Nazi and Klan groups to revisionists and Christian Identity groups. Indeed, the Museum of Tolerance's special map called "the Other American" has attracted more than 750,000 visitors since the Museum opened.

The Center also houses a National Task Force on hate and works closely with law enforcement agencies and has pioneered an innovative program called Tools for Tolerance. Indeed, it was to the latter program that Federal prosecutors, in a plea agreement with members of the 4th Reich skinhead group, arranged for this group, which had been charged in planning to bomb the AME Church in Los Angeles, to visit the Museum and to participate in its special programs.

Mr. Chairman, let me begin by reading to you something that came off the Internet a few days ago. "We need to begin the revolution now, without delay. Hopefully you all know the revolution of which I speak. The revolution to cleanse our grand nation of the undesirables (niggers, beans, jews, the like) and return the white man to his rightful place atop america.

The Oklahoma City bombing was a government setup to discredit the militias and whi(t)e activists. We need to begin our fight to eradicate the Federal Government, dominated by Jews since the 30's, beholden to the NAACP and alike organizations. If we do not act soon, we will let america slip into the doldrums of racial equality. I am by no means crazy, just realistic. The white man, superior to all, as I hope you realize, needs to assert his power. I will be leading my mil(i)tia in southern califronia [California] against targets in the southwest. Join me to free america!!"

Mr. Chairman, in sense this statement posted on May 7, 1995 by a self-proclaimed racist militiaman summarizes why we are here today. First, permit me a brief comment on the militias themselves—are they a threat to America? The only conclusion you can reach after reading manuals like those distributed by the militia of Montana is yes, they intend to be a threat to this country. When a man stands before you and says that he hates everything you stand for and wants to kill you and has a gun in his hand, he is certainly a threat. These groups encourage their followers to prepare for a self-prophesied doomsday scenario and gives the specifics of how to hasten it. Assaults on the most vulnerable targets, such as commercial and industrial enterprises, police stations, government property, mass communication media, ships, trains and planes. Liberation of prisoners and creation of riots in penal institutions; kidnapping of renowned artists and sports figures; acts of sabotage, particularly on firms and properties not owned by Americans. Their intentions are only dangerous to Society if they have free access to weapons and explosives. Access to the detail of construction of such bombs is provided in the manual and on the Internet.

The manual accuses the Federal Government of controlling education and the press and regularly using the Internal Revenue Service to spy. Even before Waco, the manual details on escalating series of "Alerts" which could lead to the inevitable, violet confrontation with Federal law enforcement officers.

Mr. Chairman, today it's militias. Tomorrow it could be their own courts and senates and their own commander-in-chief. America cannot and should not tolerate private armies, they are a recipe for potential anarchy, violence and civil disorder.

More specifically Mr. Chairman, on the issue of the Internet, the Wiesenthal center has located, both prior to and since the Oklahoma massacre, numerous 'recipes' for building bombs. Information once only available behind the counter of a few counterculture bookstores is now being promoted into millions of homes in America on a daily basis. Under our system of laws and freedoms, we are unable to stop the flow of such dangerous information to people bent on destruction. But America, can and must, prohibit the over-the-counter sale of large quantities of chemicals like ammonium nitrate and other explosives or toxic substances to people who have no legitimate use for them. A licensing procedure would at least make it more difficult for potential terrorists to anonymously carry out their plans.

While the Wiesenthal Center endorses the President's Anti-Terrorism Legislation, we believe that in view of the bombings at the World Trade Center and Oklahoma City that the consideration of controls on sales of such items be considered by Congress with all deliberate speed and not the one-year period suggested in Section 103 of the President's bill.

Mr. Chairman, the threat I quoted in my opening remarks follows a pattern evident since last year's increase in hi-tech traffic by America's hate groups. By early 1995 the Wiesenthal Center has logged over 50 such groups utilizing various elements of cyberspace—from electronic bulletin boards to sophisticated WEB-sites on the Internet.

The reasons for this troubling trend are quite clear. Cyberspace offers direct instantaneous, cheap, mainstream communications in the marketplace of ideas. Further, young people—a target group for racists are especially drawn to this cutting edge of technology.

Cyberspace has suddenly empowered marginal local groups, be they overt White Supremacists or militias with racist ties like the Northern Regional Militia of Michigan who market nationally, inflammatory videos and computerized files which fuel a conspiratorial, rabidly anti-government and often violent world view.

It also empowers local militia and hate group members with a sense that they are part of an increasingly powerful, nationwide movement. In addition to the obvious mainstream marketing capabilities, available technology also permits, when desired, anonymity when launching hate attacks on the internet.

So what can or should be done with a decentralized network of more than 50,000 interconnected networks flowing to some 30 million computers? First, if nothing else, we need to give law enforcement, Federal and local, the opportunity and capability to monitor hate and violence-oriented postings in cyberspace. Whether hate groups or militias with racist ties, authorities will be unable to effectively keep tabs on trends and potentially illegal activity if they cannot do the equivalent of clipping a newspaper article by downloading a file.

We are not advocating an attack on the first amendment freedom of Americans, however, we do believe that law enforcement should be free to investigate clearly expressed intentions to commit violence as was expressed in the statement I quoted from at the beginning of my comments. Secondly, we also need the attention and leadership of the technology providers to help America marginalize the hate-mongers.

Mr. Chairman, as you know, on-line and Internet access providers sell a service to the public and we are happy to report that in some cases these providers are already taking a pro-active stand to bar their services from such hate-mongers.

Third, in evaluating any potential course of action we need to look at the particular format and function of the use of the hi-tech superhighway to see what limits—if any should be applied. So, for example, we need to keep in mind that the obscene or threatening phone caller has neither his privacy nor his speech protected when he threatens a member of the community via the phone—why are those protections afforded if he launches the same attach via the Internet?

Mr. Chairman, tradition, community standards, truth-in advertising and other considerations mean that today neither CNN nor the Washington Post is likely to accept advertising from avowed racists or Nazis. The Wiesenthal Center hopes that the community of on-line providers will develop their own guidelines for access to electronic publishing and advertising just as other forms of communication in our society have.

Finally, Mr. Chairman, the Simon Wiesenthal Center and its Museum of Tolerance is dedicated to reaching and changing people who harbor racist views, but not everyone is reachable. In those cases every effort must be made to keep the means for mass destruction out of the hands of future Tim McVeighs.[1]

Senator SPECTER. Thank you very much, Rabbi Hier. Thank you.

Mr. Robert Litt, Deputy Attorney General, Criminal Division, U.S. Department of Justice.

Welcome, Mr. Litt, and the floor is yours.

STATEMENT OF ROBERT S. LITT, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. LITT. Thank you. Mr Chairman, Senator Kohl, members of the subcommittee, the horrible tragedy in Oklahoma City has focused the attention of this subcommittee and the Department of Justice on domestic and international acts of terrorism.

As President Clinton has said, "It is not enough to prosecute the guilty, if we cannot protect the innocent." Our task in this regard is all the more difficult because we live in an open society that is firmly committed to the protection of constitutional rights.

Atrocious acts of violence like the Oklahoma City bombing are facilitated by the free flow of information in our country. As you noted, Mr. Chairman, and Senator Kohl and Rabbi Hier, the information superhighway does not only carry information about government, business, and personal matters. It is also home to all manner of violent hate groups.

Information on how to build bombs is freely available on the Internet and on other public and private computer bulletin boards. And Mr. Chairman, you gave a couple of examples of that.

Because of press coverage after the Oklahoma City bombing, most Americans—including those few among us who are inclined to acts of violence—now know that bombs can be made from commonly available materials and that manuals on how to do this are widely available.

In fact, similar guides have been available in bookstores and public libraries for many years and are still available there, today. But, the Internet has unquestionably increased the flow of this information, which is now easily available to millions of people.

Anyone can learn how to make a murderous bomb in the privacy of his own home, untroubled by the constraints that he might feel

[1] Supporting documents submitted by Rabbi Hier are retained in the committee files.

normally about going into his local bookstores and asking for a bomb cookbook.

People who distribute information of this sort are absolutely contemptible in the callous disregard that they show for the safety of their fellow citizens. In my view, there is absolutely no justification for posting the sort of material on the Internet that you read, Mr. Chairman.

The implications of these actions are frightening because not only do would-be terrorists have access to detailed information on how to construct explosives, but so do children. And as Senator Kohl noted, there are instances all the time of children with access to this information making bombs and, frequently, maiming or killing themselves.

This problem can only grown worse as more families join the Internet.

How can we deal with the dangers that are posed by the wide, online dissemination of information about how to make bombs? There are a number of Federal laws already on the books which we can use to prosecute bomb-related offenses. These include laws relating to extortion, making threats, conspiracy, and aiding and abetting the violation of other Federal laws, and these laws can be applied even when the offense in question is carried out through speaking.

Similarly, there is a specific statute on the books, section 231 of title XVIII, that specifically prohibits demonstrating or teaching how to make an explosive device with the intent of knowledge that this device will be used in a civil disorder, which is defined in the statute.

These criminal laws apply with the exact same force on the Internet. For example, if a group used the Internet to plan the bombing of a building or communicated genuine threats to engage in such attack, they would be prosecuted.

We can, therefore, clearly act to punish conduct that falls within the scope of the existing Federal laws. But when we address speech, the power of law enforcement is limited by the first amendment to the Constitution.

As the members of this subcommittee well know, we must guard the public's right to free speech, even while protecting that public from criminal activity.

In my prepared remarks, I discuss the relevant law in more detail. The basic legal principle is clear. The first amendment protects speech, even speech that advocates or teaches illegal action, unless there is an imminent danger of, and an incitement to, lawless action, or unless the speech itself constitutes a crime.

Speech that does not meet this standard is protected under the first amendment. The sick people who use the Internet to distribute information on how to construct bombs are quite aware of the constitutional limitations prosecutors face.

Senator Specter, you noted the posting on the Internet which said, "this is for informational purposes only." Although this language is a transparent attempt to conceal the writer's true intentions, it may have legal effect, as court's may rely on these disclaimers or warnings.

I assure that the Department of Justice takes the threat of violence facilitated by the Internet very seriously. If and when we are faced with a case in which the facts justify prosecution within constitutional limits, we will act swiftly and diligently to protect the public.

Already, we have not hesitated to prosecute criminal activity on the Internet, whether it be the distribution of child pornography or the sending of threats. But the first amendment applies to speech on the Internet, as well as on the street corners; to bomb manuals posted on electronic bulletin boards, as well as bomb manuals for sale in corner bookstores. All of these are protected by the first amendment, unless they constitute direct incitement to carry out illegal activity or, for example, the person making the statement actually conspires in or aids and abets in the making of terrorist bombs.

In other circumstances, we—as well as the Congress—are restrained by the Constitution from punishing speech, no matter how repugnant or potentially harmful it is.

However, more can be done within constitutional limits to punish terrorist and violent activity occurring on the Internet. President Clinton has recently proposed important new authority in the Omnibus Counterterrorism Act of 1995 and the Antiterrorism Amendments Act of 1995, which would fill some gaps in Federal criminal legislation regarding terrorism.

By requiring the inclusion of taggants in explosive materials, these bills would greatly increase our ability to investigate and prosecute bombmaking and would thereby deter terrorists who now feel safe in the anonymity of their awful actions.

Senator SPECTER. Mr. Litt, would you summarize the balance, please?

Mr. LITT. Yes; I will, I am coming right to the end, Mr. Chairman.

The legislation would also require a study of ways to neutralize commonly available precursor chemicals such as those used in Oklahoma City and New York, to prevent their use as explosives, and contains important procedural reforms that would help us prevent and prosecute terrorist activity without limiting our freedom of speech.

My prepared remarks also address the subjects of encryption and anonymity on the Internet, which are also extremely important to our ability to investigate these criminal activities and I would simply refer to them and urge this subcommittee to continue to work on these issues and we will continue to work with you to address them.

Thank you very much.

[The prepared statement of Mr. Litt follows:]

PREPARED STATEMENT OF ROBERT S. LITT

Mr. Chairman and members of the Committee: I appear before you today just three weeks after the Oklahoma City bombing. That horrible tragedy has again focused this Committee and the Department of Justice on domestic and international acts of terrorism. As the President has said, it is not enough to prosecute the guilty if we cannot protect the innocent in the future. Our task is all the more difficult because we live in an open society firmly committed to the protection of constitutional rights.

Atrocious acts of violence like the Oklahoma City bombing are facilitated by the free flow of information on how to construct destructive weapons. The information superhighway doesn't only carry information about government, business and personal matters. It is also home to all manner of hate groups who use it for their own purposes. For example, information on how to construct bombs is freely available on the Internet and other public and private computer bulletin boards. Press coverage of the Oklahoma City bombing has made this fact widely known. Now most Americans, including those few inclined to violence, understand that bombs can be made from commonly available materials. They also know that "how to" guides are widely available.

In fact, similar guides have been available in bookstores and public libraries for years. But the Internet has unquestionably increased the flow of this information; it is now easily available to millions of people. A person so inclined can learn how to construct a devastating bomb in the privacy of his own home, untroubled by the constraints he might normally feel about purchasing a bomb cookbook at the local bookstore.

For example, according to the Los Angeles Times, only hours after the Oklahoma City bombing, someone posted on the Internet directions for making a similar bomb, including a diagram. It also reported that a discussion group on the Internet told readers not only how best to build that type of bomb, but also how to synthesize other explosives, how to build a pipe bomb, and how to make Sarin, the nerve gas which was used in the Tokyo subway attacks. Another Internet posting offered both information on how to build bombs and details on how the Oklahoma City bomb was used "and could have been better." In some cases, information available on the Internet and elsewhere deals specifically with how to harm federal agents.

People who distribute information of this sort are contemptible in their callous disregard for the safety of their fellow citizens. The implications of their actions are frightening. Not only do would-be terrorists have access to detailed information on how to construct explosives, but so do children. The Los Angeles Times story I referred to earlier noted incidents in which teenagers were killed while trying to construct bombs by following instructions in publications. This problem can only grow worse as more families join the Internet "society."

How can we deal with the dangers posed by the wide on-line dissemination of information about how to make bombs? A number of federal laws can be used to prosecute bomb-related offenses. Laws such as those relating to extortion, threats, conspiracy, and aiding and abetting the violation of other federal laws, can be applied even when the offense is accomplished through speech. For example, last year a court in the Southern District of New York rejected a claim by Omar Ahmed Abdel Rahman that his alleged participation in a conspiracy to levy a war of urban terrorism was protected by the First Amendment. The court held that, while conspiracy often has an element of speech in its commission, speech is not protected when it is the vehicle of the crime itself. Criminal laws like the conspiracy statute apply with the same force to the Internet. If a group used the Internet to plan to bomb a federal building, or communicated real threats that they intended to engage in such an attack, they would be prosecuted.

Similarly, section 231 of Title 18 specifically prohibits demonstrating how to make an explosive device of one intends or knows that it will be used in a civil disorder involving acts of violence affecting interstate commerce. In *United States* v. *Featherston*[1] a circuit court upheld the conviction under this statute of individuals who gave instructions at a meeting on how to make and assemble explosive and incendiary devices in order to prepare the attendees for "the coming revolution." Because this presentation was to a cohesive, organized group preparing for "the coming revolution," ready to strike quickly, and including some members regularly trained in explosives, the court found no violation of the First Amendment.

We can, therefore, clearly act to punish conduct that falls within the scope of existing laws. But when we address not conduct but possibly protected speech, the power of law enforcement is restricted by the First Amendment. As the Committee well knows, we must guard the public's right to free speech even while protecting the public from criminal activity. The Constitution imposes stringent limits on our ability to punish the mere advocacy of principles or the mere dissemination of information, without more, even if the communications in question are utterly repugnant.

The Supreme Court in *Brandenburg* v. *Ohio*[2] defined the line between protected and unprotected speech concerning advocacy of illegal activity. In that case, the Court struck down as unconstitutional an Ohio statute that made it illegal to advo-

[1] 461 F.2d 1119 (5th Cir.), cert. denied, 409 U.S. 991 (1972).
[2] 395 U.S. 444 (1969).

cate "the duty, necessity, or propriety of crime, sabotage, violence, or unlawful methods of terrorism as a means of accomplishing industrial or political reform." The Court ruled unanimously that advocacy of the use of force or of illegal activity can be punished only where such advocacy is "directed to inciting or producing imminent lawless action and is likely to incite or produce such action."

The standard of *Brandenburg* v. *Ohio* protects speech even where the advocacy and "information" conveyed is of the most dangerous and offensive nature. Thus, in *Herceg* v. *Hustler Magazine,*[3] the Fifth Circuit Court of Appeals held that Hustler Magazine was not liable—even in a civil lawsuit—when a teenage boy read an article in the magazine that explained in detail the procedure known as "autoerotic asphyxia" and died by hanging while attempting to carry out the instructions. The court ruled that, however unpleasant the article was, and regardless of whether the conduct it described was illegal, the article was protected by the First Amendment because it did not incite readers to imminent lawlessness. The court examined the article in question, which included disclaimers advising readers not to try the techniques described, and concluded that "no fair reading of it can make its content advocacy, let alone incitement to engage in the practice."

As a last example of the application of the *Brandenburg* standard, I would note that we have a specific statute, the Smith Act, section 2385 of Title 18, which prohibits advocating the forcible overthrow of the government. But as with other statutes, this statute cannot be used to prosecute mere speech. In *Yates* v. *United States,*[4] the Supreme Court held that the Smith Act may not be used to prosecute advocacy alone.

Thus, the legal principles involved are clear. The first Amendment protects speech—even speech that advocates or instructs illegal action—unless there is an imminent danger of, and an incitement to, lawless action, or unless the speech itself constitutes a crime. No criminal statute can constitutionally be applied to speech that does not meet this standard.

The same rules apply to information communicated over the Internet. As I note before, individuals who actually agree to commit a bombing, or threaten to do so, can be prosecuted for conspiracy or threats. Moreover, we can prosecute individuals under 18 U.S.C. § 231 for showing how to make a bomb if they know it will be used in a civil disorder, as defined in the statute. But not federal statute today covers the widespread distribution of information about making a bomb, without more, and, to pass constitutional muster, any such statute would have to require, for example, that the defendant intended or knew that the information would be used in illegal activity, or intended to incite imminent lawlessness.

The people who use the Internet to distribute information on how to construct bombs are quite aware of the constitutional limitations prosecutors face. To protect themselves from prosecution they will state, for example, that they supply instructions on how to construct a bomb "solely for informative purposes." The Internet posting I mentioned earlier, offering information on how the Oklahoma City bomb "could have been better," contained such a disclaimer. Although such language is a transparent attempt to conceal true intentions, it may have legal effect, as courts may rely on disclaimers or warnings to show that no incitement was intended.

In sum, it is generally not possible to penalize speech unless the speech crosses the line from providing information or mere advocacy to inciting imminent lawlessness or participation by the speaker in illegality. This protection applies to speech on the Internet as well as on the street corners; to bomb manuals posted on electronic bulletin boards as well as bomb manuals for sale in corner bookstores. All are equally protected by the First Amendment, unless they constitute direct incitement to carry out illegal activity, or the publisher, for example, conspires in or aids and abets making the bombs.

I assure you that the Department of Justice takes the threat of violence facilitated by the Internet very seriously. If we are faced with a case in which the facts justify prosecution within constitutionally permissible limits, we shall act swiftly and diligently to protect the public. Indeed, we have not hesitated to prosecute criminal activity on the Internet, whether it be distribution of child pornography or the sending of threats. But, in other circumstances, we, as well as Congress, are constrained by the Constitution from taking any action to penalize speech, no matter how distasteful or apparently harmful.

However, more could be done within constitutionally permissible limits to punish terrorist and violent activity occurring on the Internet. While we cannot prohibit speech that does not rise to inciting imminent lawless action, expansion of the scope

---

[3] 814 F.2d 1017 (5th Cir. 1987), cert. denied, 485 U.S. 959 (1988).

[4] 354 U.S. 298 (1957), overruled in part on other grounds, *Burks* v. *United States,* 437 U.S. 1 (1978).

of federal criminal laws with violent, terrorist activity will permit the Department of Justice to prosecute those who engage in efforts to assist violence and terrorism over the Internet. President Clinton has recently proposed important new authority in this area, in the Omnibus Counterterrorism Act of 1995 and the Antiterrorism Amendments Act of 1995. These bills would fill some gaps in federal criminal legislation regarding terrorism. By requiring the inclusion of taggants in explosive materials, the bills would greatly increase our ability to investigate and prosecute bombmaking—and thus deter those who seek to commit terrorist acts. Similarly, the legislation would require a study of ways to neutralize commonly available precursor chemicals such as those used in the bombing in Oklahoma City and New York, to prevent their use as explosives. The legislation also expands federal jurisdiction over terrorist activity, and amends immigration law to facilitate the deportation of foreign terrorists.

Futhermore, the investigatory reforms and initiatives in those bills, such as allowing access to credit records through appropriate legal procedures and expanding the list of felonies that can be used as the basis for court-ordered electronic surveillance, will permit the government to better track and prosecute those who misuse information available on the Internet or in the bookstore. Without limiting our freedom of speech, these proposals would help us prevent and prosecute terrorist activity.

Of particular importance is funding the Digital Telephony bill passed by Congress last session. This issue is central for ensuring the practical availability of court-authorized law enforcement electronic surveillance of digitized communications.

In addition, as Director Freeh pointed out in his statements before the House Judiciary Committee on April 6th, power encryption is becoming more commonplace. Drug cartels and other criminals are already buying sophisticated communications equipment. Director Freeh noted that, unless the encryption issue is adequately addressed, criminal communications over the telephone or the Internet will be encrypted and inaccessible to law enforcement even if a court has approved electronic surveillance. He noted then, and again before the House Subcommittee on Crime, that we must continue working to address this problem.

Crime on the Internet also presents the critical issue of anonymity, which is related to encryption. The development of secure, anonymous electronic mail will greatly impair the ability of law enforcement to track terrorist communications. For example, one Internet posting regarding the Oklahoma City bombing and bomb construction was sent through an "anonymous remailer"—a device designed to forward electronic mail so that the original sender is unknown—probably to prevent tracing. Computer and law enforcement experts are currently debating to what extent anonymous communications should be permitted, and how to balance a law-abiding person's legitimate need for anonymity with society's need to hold individuals accountable for their activity.

Supporters of anonymous communications note, correctly, that anonymity supports legitimate activities. It allows whistleblowers to come forward without fear of retribution. It permits individuals to communicate without sacrificing personal privacy—for example, a group of rape victims might wish to communicate with each other without being personally identified. These advocates also point out that other technologies, most notably the telephone and mail systems, have long allowed for anonymous communications.

Others contend that such absolute anonymity is unacceptable, and emphasize the importance of accountability. While not disputing the benefits of anonymous communications, they note that criminals often rely on those benefits. Although prior communication methods permit anonymous communications, those services generally provide one-to-one communications. It would be both time-consuming and costly to use either the phone or mail systems to disseminate information wholesale, effectively preventing wide-scale malicious use and limiting the harm that can be caused. On the Internet, by contrast, there are no monetary or technical impediments to worldwide dissemination of communications. Anonymous, worldwide dissemination of terrorist information must be of paramount concern to law enforcement and to ordinary citizens.

We believe that it is possible to deal with both of these issues—encryption and anonymity. Privacy rights should generally be protected, but society should continue to have, under appropriate safeguards and when necessary for law enforcement, the ability to identify people and hold them accountable for their conduct. In the case of encryption, the appropriate balance can be achieved by the widespread use of reliable, strong cryptography that allows for government access, with appropriate restrictions, in criminal investigations and for national security purposes. The federal escrowed encryption standard issued last year is designed to achieve this delicate balance for voice telephony.

In the case of anonymity, the middle ground between total anonymity and accountability is confidentiality. In this context, confidentiality means that the identity of an individual can be ascertained, but only in appropriate cases and, perhaps, only pursuant to legal compulsion through a judicially-supervised process. We will have to diligently study the developing technology in this area in order to ensure that laws continue to properly balance the needs of law enforcement with privacy concerns.

Mr. Chairman, I thank you for the opportunity to appear before you today. The Attorney General and the Department of Justice will work with the Congress to meet the challenge of terrorism. We must, however, fight terrorism without infringing the constitutional rights of our citizens. As the Deputy Attorney General stated to the Subcommittee on Crime of the House Judiciary Committee on May 3rd, the choice between civil liberties and a safe society is a false choice. We cannot trade off the guarantees of the Bill of Rights in order to uphold our duty to "insure domestic Tranquility." We look forward to working with you and the Congress on the issues.

Senator SPECTER. Thank you very much, Mr. Litt.

We now turn to Mr. William Burrington, assistant general counsel and director of government affairs, America Online, Inc.

Welcome Mr. Burrington, the floor is yours.

STATEMENT OF WILLIAM W. BURRINGTON, ASSISTANT GENERAL COUNSEL AND DIRECTOR OF GOVERNMENT AFFAIRS, AMERICA ONLINE, INC., AND CHAIRMAN OF THE ONLINE OPERATORS POLICY COMMITTEE OF THE INTERACTIVE SERVICES ASSOCIATION

Mr. BURRINGTON. Thank you, Mr. Chairman; Senators Kohl and Leahy and Feinstein.

My name is William W. Burrington. I am chairman of the Online Operators Policy Committee of the Interactive Services Association, which I will refer to as the ISA, based here in Silver Spring, MD., and I am assistant general counsel and director of government affairs, for America Online, Inc., in Vienna, VA.

I appear before you today on behalf of the ISA and its Online Operators Policy Committee, which is comprised of America Online; Apple's e-World; CompuServe; Delphi Internet Services Corp.; Genie; Interchange Network Co.; MCI; Microsoft Network; Prodigy Services Co.; and Ziff Davis Interactive, essentially the consumer online industry.

We understand that the purpose of these hearings is to discuss interactive online services, including those that provide access to the Internet; the legal and constitutional framework in which they exist; and the concern for terrorism and other illegal activities on such services.

We are here because we want to work with you to maximize the good that this new publishing and communications medium can provide and explain the need to maximize the free flow of information and protect the interests of a free and safe society.

Let me make it very clear at the outset that our industry strongly opposes illegal activity over our networks. We have an active working relationship with law enforcement at all levels to help them to the extent legally permissible and we have all taken self-regulatory actions to keep the networks clean.

We oppose illegal activities for two fundamental policy reasons. First, as responsible corporate citizens, it is our duty and obligation to do so. Second, we have a great vision for the networks of the fu-

ture and want them to be open and hospitable, not scary and not dangerous.

We believe that we can do this and still protect the first amendment and protect the interests of our customers in their communications. This is a delicate balance and we look forward to working with you, Mr. Chairman, and your subcommittee to find a solution.

While online services can be among the sources of information that people may not agree with, they also offer a unique outlet for positive, social responsibility and action. For example, following the tragic circumstances of Oklahoma City, the new Online and Internet communities were able to respond immediately in an extremely positive way to establish communications and provide information to those involved in that disaster.

At my company, for example, America Online, within minutes of the Oklahoma City bombing, our news department set up a special Oklahoma City news area on our service. Hundreds of thousands of members entered this special new area on the day of the disaster and in the weeks which followed.

The area devoted a section to the American Red Cross Disaster Relief Services Fund and allowed our members to make direct contributions to the Red Cross. The national outpouring of support for the people of Oklahoma City was not only evident in Oklahoma City, itself, but it was freely expressed by literally hundreds of thousands of Online users throughout the United States and in other countries, as well.

Currently, there are over 7 million subscribers to PC-based online services, with subscriber growth at 25 percent or more per year for the last few years, and that trend is continuing.

All of these online services now provide, or soon will provide, their subscribers with broad access to the Internet. Complementing the online services are the estimated 50,000-plus bulletin boards being operated by companies for customer or employee support, entrepreneurs, and hobbyists.

The owners of the boards are a diverse lot, so any policies governing the behavior of their users are quite diverse.

Then, there is the Internet. The Internet is essentially a set of protocols that enable computers to be connected to each other for purposes of sharing information and facilitating personal communications. The Internet is a world-wide phenomenon, available in over 90 countries, connecting some 5 million different computer systems and accessed by an estimated 10 to 30 million people.

This system of connected computers is fast becoming a ubiquitous communications service available to the general public, not only nationwide, but globally. Because of the Internet's diversity, there is no central governing body or policy governing user behavior. It is left to the individual systems. At best, user behavior is self-governed by the general user community based on the loose principles of what we call netiquette.

One of the many benefits of online services is that they break the boundaries of gender, age, race, religion, political affiliation, or lifestyle orientation, and that they bring together people who are separated by geography, whether rivers or oceans, to share common interests.

Online forums have been established, for example, for people interested in specific types of computers, for senior citizens, and people with disabilities. Interactive services empower their users. Tools provided by interactive services can act as an extension of the person, compensating for different abilities related to, for example, age or physical health. Electronic grocery shopping, for example, can be a lifeline to a homebound individual who is seeking to stay independent.

Communities, too, will experience increasing social and political empowerment through electronic communications forums. More than anything else, people use online services to communicate both privately and publicly across America as well as around the globe.

Senator SPECTER. Mr. Burrington, could you summarize, please?

Mr. BURRINGTON. Yes, I knew that was coming. [Laughter.]

Let me summarize, and I will just go right to the end, here, and I do urge the full committee to look at our full testimony.

As this subcommittee and other policy makers consider policy for online services, it is important that they take into consideration the following realities of this new medium. The sheer size of online services where millions of private messages and hundreds of thousands of public postings on bulletin boards make it impossible for the operators of these services to knowingly be aware of and screen everything that is on their system.

Second, because of this empowerment to the public, the originator of the content, whether it is an individual or a corporation, must be held responsible for the content it places on any online service, not the operator or provider of the system on which the content is placed, unless that operator had editorial control or the intent to participate in illegal activity.

And finally, online services and the Internet are a global medium and any rule set for this country will not necessarily apply to those services located outside of the United States but easily accessible by Americans residing in the United States Perhaps more than any other medium that has ever been used by Americans, online services support the fundamentals of our participatory democracy.

Our Government's role should be to facilitate, not to inhibit, the development of the national and global information infrastructure. That has what Government has done so far.

If America's values teach us anything, it is that, particularly at times like these, what we need to foster is more speech, not less.

Thank you very much, Mr. Chairman.

[The prepared statement of Mr. Burrington follows:]

PREPARED STATEMENT OF WILLIAM W. BURRINGTON

Mr. Chairman and members of the Subcommittee, I am William W. Burrington, Chairman of the Online Operators Policy Committee of the Interactive Services Association and Assistant General Counsel and Director of Government Affairs for America Online, Inc. in Vienna, Virginia. I appear before you today on behalf of the Interactive Services Association ("ISA") and its Online Operators Policy Committee.[1]

We understand that the purpose of these hearings is to discuss interactive online services, including those that provide access to the Internet, the legal and constitu-

[1] ISA's Online Operators Policy Committee is comprised of: America Online, Inc.; Apple e-World; CompuServe; Delphi Internet Services Corp.; GEnie; Interchange Network Company; MCI; Microsoft Network; Prodigy Services Company; and Ziff Davis Interactive.

tional framework in which they exist, and the concern for terrorism and other illegal activities on such services.

We also understand that questions are being raised concerning the nature of some conversations that are on the "NET." We want to work with you to maximize the good that this new publishing and communications medium can provide and explain the need to maximize the free flow of information and protect the interests of a free and safe society.

For example, following the tragic circumstances of Oklahoma City and other disasters like the Los Angeles earthquake of 1994, the new online and Internet communities were able to respond immediately in an extremely positive way to establish communications and provide information in an entirely new way to those involved in that disaster. At America Online, for example, within minutes of the Oklahoma City bombing our news department set up a special Oklahoma City news area on our service. Hundreds of thousands of our members entered this special news area on the day of the disaster and in the weeks which followed. The area devoted a section of the American Red Cross Disaster Relief Services and allowed our members to make direct contributions to the Red Cross. The area also featured up-to-the -minute news and information, fifteen (15) chat rooms for members to exchange news and views about the tragedy, a message board, and live coverage from NBC's Oklahoma City affiliate. The national outpouring of support for the people of Oklahoma City was not only evident in Oklahoma City itself, but it was freely expressed by literally hundreds of thousands of online users throughout the United States and in other countries as well.

The First Amendment protects speech on an electronic service just as it protects speech disseminated via cable television services and, to a somewhat lesser extent, broadcast media. This means that the government cannot directly or through court action limit speech or require that a certain type of speech by carried by those services. Of course, such protection is not absolute and speech that is obscene or defamatory may be restricted in certain circumstances. Nor does the First Amendment protect speech that moves from expression to action (e.g., Holmes' yelling "fire" falsely in a crowded movie theatre).

What complicates this inquiry is that we cannot stop with a discussion of publishing or dissemination and the First Amendment. A good deal of the services offered by our members are dedicated to the facilitation of communications between individuals. These may be in the form of electronic mail ("e-mail") or bulletin boards run by others or other electronic communications. In these communications services, we are not publishing, we are providing others with the means to communicate and to publish. To the extent that we look at these as communication services, there is also constitutional protection (Fourth Amendment) for individuals to have a reasonable expectation of privacy in communications. This constitutional protection was significantly expanded to cover digital electronic communications under the Electronic Communications Privacy Act of 1986.

Therefore, in the best sense of citizenship we have both rights (First Amendment) and responsibilities (duty to protect private communications from unauthorized access) in the provision of online and internet services.

Let me say at the very outset that our industry strongly opposes illegal activity over our networks. We have an active working relationship with law enforcement at all levels to help them to the extent legally permissible, and we have all taken self-regulatory actions to keep the networks "clean."[2] We oppose illegal activities for two fundamental policy reasons. First, as responsible corporate citizens it is our duty and obligation to do so. Second, we have a great vision for the networks of the future and want them to be open and hospitable and not scary and dangerous. We believe. We believe that we can do this and still protect the First Amendment and protect the interests of our customers in their communications. This is a delicate balance and we look forward to working with this subcommittee to find the solution.

As the oldest non-profit North American association serving businesses that deliver telecommunications-based interactive services to consumers, the ISA has been responsive to concerns about the social and political impact of this new interactive medium that millions of Americans use very day. ISA's 300-plus members (see Appendix B) represent the full spectrum of industries now active in delivering personal interactive services. ISA's membership includes companies from the advertising,

[2] For example, members of ISA, in conjunction with the National Center for Missing and Exploited Children, prepared a pamphlet called "Child Safety on the Information Highway." The pamphlet provides guidance for parents and children about safe and productive online experiences. A print version of the pamphlet (which is also available online) is attached as Appendix A.

broadcasting, cable, computer, financial services, marketing, publishing, telephone, and travel industries.

When it was formed in 1981, the ISA and its members had a vision that interactive service would be as common to American consumers as broadcast television and the telephone had become. Back in the early 80s, very few Americans knew anything about interactive services, online communications, or even what a modem was; and of course the Internet was unheard of. In fact, it has only been in the last two years that extensive public awareness of our industry has occurred. While important strides have been made for transforming the ISA's vision into reality during the past 13 years, the industry still has a way to go before our mass-market vision is fully realized. But our industry firmly believes that the vision is well on its way to becoming reality.

In may testimony today, I would like to discuss three points with the subcommittee:

First, an overview of the interactive services marketplace, which includes online services and the Internet;

Second, a review of the benefits of online services and the importance of communications to this new medium; and

Third, a discussion of the legal framework supporting online services and how best to support the interest of privacy and freedom.

INTERACTIVE SERVICES NATIONALLY AND GLOBALLY

During the last few years there has been a blossoming awareness and use of national and global interactive services. The ISA defines "interactive services" as easy-to-use, telecommunications-based services designed for information exchange, communications, transactions, and entertainment. These services today are accessed by a personal computer (PC), telephone, screen telephone, or television and are for personal use, both in the home and the office. Today, the PC with a modem connected to a telephone line is by far the primary way in which consumers access screen-based interactive or online services.

Online services

While technologically similar and sometimes marketed together, online services fall into three different product areas—commercial services such as America Online, bulletin boards, and the Internet. The services are differentiated by their management. While these products raise distinct issues, they often are provided to the consumer in an integrate manner. An online computer network, in addition to offering its own services, typically provides access to and tools to more easily use the Internet as well as bulletin boards run by third parties.

Currently, there are over 7 million subscribers to PC-based online service that are likely to generate $1 billion annually in subscription, transaction, and advertising fees. The more widely used online services include America Online, Apple's e-World, CompuServe, Delphi Internet Services, GEnie, and Prodigy. Subscriber growth has been occurring at a rate of 25 percent of more per year for the last few years. In fact, during the first quarter of 1995, it is estimate the number of subscribers to these services grew by over 1 million.

These online services are owned by companies that package technology and a broad range of services to present a uniform system that consumers subscribe to for a monthly fee and/or hourly usage fees. These online computer networks often have established policies that specify what kind of user behavior is acceptable when using the service. Subscribers who violate these policies can be and are removed from the services. All of these online services now provide or will soon provide their subscribers with broad access to the Internet.

Complementing the online services are the estimated 50,000-plus bulletin boards being operated by companies for customer or employee support, entrepreneurs, and hobbyists. Theses bulletin boards usually are PCs with phone lines connected to them so that people can access the information housed on the PCs. In many ways bulletin boards are mini commercial services. Many of these bulletin boards are free. And because the owners of the boards are a diverse lot, the policies governing the behavior of their users, when they do exist, are quite diverse.

Then there is the Internet. The Internet is essentially a set of protocols that enable computers to be connected to each other for purposes of sharing information and facilitating personal communications. The Internet is a world-wide phenomenon available in over 90 countries (160 when e-mail only is included), connecting some 5 million different computer systems, and accessed by an estimated 10–30 million people. These connected computer systems are operated by universities and other nonprofits, research institutions, governments, businesses, and individuals, Because

of the Internet's diversity, there is no central governing body or policy governing user behavior. It is left to the individual systems. At best, user behavior is self governed by the general user community based on the loose principles of "netiquette."

A user can access the Internet in a variety of ways. Traditionally Internet access was provided by universities, government and research organizations. Access was supported by nonprofit groups and the U.S. and state government. There are now many online service providers that offer Internet access to companies and to individuals as a single service. These companies are called Internet service providers ("ISPs"). Services like America Online, CompuServe, and Prodigy also provide Internet access as a feature of their systems. Even bulletin board operators can and do provide Internet access. Any person on a public e-mail system can send e-mail through the Internet. Certain Bell operating companies are now seeking to provide Internet access. Internet access is fast becoming a ubiquitous communication service available to the general public, not only nationwide, but globally.

Applications

The most popular interactive or online services fall into five general categories. Consumers look to interactive services to bring them:

1. Fast changing information (e.g., news, sports scores, financial services, and directories);
2. Electronic communications (e.g., news, sport scores, financial services, and directories);
3. Transactional services (e.g., banking, grocery shopping, travel reservations, and other product shopping);
4. Entertainment (e.g., games—especially multi-user games, horoscopes, movie reviews, and soon movies and other video programs on demand); and
5. Computing (e.g., because online services are accessed by the personal computer, one of the most frequently used applications is seeking help with regard to the operations of one's personal computer, both for the hardware and software).

But more than anything else, people use online services to communicate, both privately and publicly. In the past three online surveys (1991–1994) conducted by the ISA with the cooperation of the commercial online services, two of the top four applications used by online users surveyed were communications applications. These two were electronic mail and communicating with others who share similar interests and hobbies.

Millions of private electronic messages are being sent every day online. Hundreds of thousands of messages are being posted on hundreds, if not thousands, of public boards covering a wide range of topics. Still other individuals are participating in real time chat well-known people in business, entertainment, and government, or just chatting with their peers from around the country on a common area of interest. People just like to talk with their fingers at the keyboard.

The networks for interactivity

In addition to the variety of devices and the technologies they will employ to access interactive or online services, American consumers also will access online services from a variety of networks originating here and abroad. While the first dozen years of consumer interactive services have relied on the regular telephone network, the next decade promises to bring a wide variety of network delivery options, including the twisted pair of today's telephone network, the coax of cable, fiber, over-the-air spectrum, and hybrids of these different approaches.

For the consumer, the type of network employed is irrelevant. Rather, the consumer wants to be able to rely on the devices they purchase to access at anytime and anyplace the services they need at affordable and predictable prices. However, the type of network will be critical to the industry during the next years in determining the array of services (voice, text, graphics, or video) that can be delivered to the kinds of devices (PC, television, screen telephone, or personal assistant) Americans will be using.

THE BENEFITS OF ONLINE

The ability to access and successfully use a variety of information will increase the productivity and enjoyment of our citizens' work, education, and entertainment. For example, interactive television services will bring entertainment to the fingertips of consumers and will provide video and other programming on demand. Currently, online services enable millions of people to communicate with each other and to access news, weather, sports, and financial information through the touch of a keyboard. These services enable communication across America as well as around the globe.

One of the many benefits of online services is that they break the boundaries of gender, age, race, religion, political affiliation, or lifestyle orientation and that they bring together people who are separated by geography—whether rivers or oceans—to share common interests. For example, many current interactive services offer online clubs. People of similar interests exchange information, participate in discussions through public messages, or chat and conference with each other online. Online forums exist, for example, for people interested in specific types of computers, programming, and software. They also exist to help people address personal needs. Forums have been established for senior citizens, people with disabilities, and alcoholics anonymous to name a few.

Interactive services empower their users. Since the beginning of consumer online services in the early 80s, one key fact has emerged and is often overlooked. Tools provided by interactive services can act as an extension of the person, compensating for differing abilities related to, for example, age of physical health. Electronic grocery shopping can be both a convenience to many, and a lifeline to a homebound individual who is seeking to stay independent. Communities too will experience increasing social and political empowerment through electronic communication, forums, information sharing, and collaborative planning. Perhaps more than any other medium that has been used by American citizens, interactive services, online services, support the fundamental principles of our democracy. And as services evolve to multimedia presentation, so too will applications tailored to those of us with hearing, speech, sight, mobility or other challenges.

Managing the risks

While this empowerment provides benefits to Americans, with it comes the ability for a few to abuse this new medium as they have with other media. Hate groups may use this new medium to promote their misguided views on races and religion. Pornographers may disseminate obscene literature and images around the world through the Internet. And irresponsible individuals may knowingly provide software and other content in violation of copyright laws.

With the advent of any new medium comes the challenge for a society to develop rules on how that medium is to be used to ensure that the full benefits are realized by a majority of its citizens. Today's hearing is an important step in our country's efforts to determine the appropriate rules for online services to operate in the United States.

As this subcommittee and other policy makers consider appropriate policies for online services, it is important that they take into consideration the following realities of this new medium:

1. The sheer size of online services, where millions of private messages and hundreds of thousands of public postings on bulletin boards, makes it impossible for the operators of these services to knowingly be aware of and screen everything that is on their systems;

2. Because of this empowerment to the public, the originator of the content, whether it is an individual or a company, must be held responsible for the content it places on any online service, not the operator or carrier of the system on which the content is placed, unless the operator had editorial control or the intent to participate in an illegal activity; and

3. Online services and the Internet are a global medium, and any rules set for this country will not necessarily apply to those services located outside of the United States but easily accessible by Americans residing in the U.S.

LEGAL PRECEDENTS FOR THE INTERACTIVE MEDIUM

In providing user communications services, online computer networks serve two separate functions: (i) publication or dissemination and (ii) user communications. The legal analysis will vary according to the functionality in which the network is engaged.

First, with regard to online conferences or bulletin board messages run by them, online computer networks provide forums for discussions on specific topics. In choosing topics for online conferences or bulletin boards and facilitating subscriber participation in them, online computer networks provide forums—such as letters to the editor or guest columnist secitons—for opinion and discussion. Their activities also are similar to those of libraries, bookstores, and newsstands, which choose the titles of books and other publications they offer patrons and customers.

It is in managing subscriber participation in online conferences and bulletin boards that online services may be able to set policies for conduct and exercise greater control over user behavior. For example, with regard to bulletin boards or conferences they sponsor, online services can require that messages transmitted for

posting be relevant to the subject of these activities. If the topic of a bulletin board or conference is the 1996 presidential election, for instance, then an online service provider could remove the posting of a message on Italian cooking for breach of its terms of services.

Second, with regard to electronic mail and private bulletin boards, online computer networks act as facilitators of private communications. In providing electronic communication facilities, they act in some respects like common carriers that must transmit communications of paid subscribers regardless of the message's content. Like telephone companies that do not get to choose which telephone calls they will retransmit and which they won't, online computer networks merely process the private electronic mail of their subscribers.

With few exceptions, online services cannot control or police how subscribers use e-mail services. Rather, they are required by law to protect the subscriber's reasonable expectations of privacy. For example, an online computer network could prohibit the use of its e-mail services to send unsolicited commercial messages. While it cannot monitor the content of e-mail messages, the online computer network could—upon receiving a complaint—act against the sender for breach of the operating rules. And, of course, upon being served with valid legal process, it could assist law enforcement officials investigating a subscriber suspected of using the e-mail system for unlawful purposes.

First amendment protections

There is no doubt that the first amendment protects the activities of online computer networks in furnishing online conferences and bulletin boards. Just like they extended from newspapers and magazines to broadcast media and, more recently, cable television, the first amendment guarantees apply to online computer networks when performing speech distribution.

The U.S. Supreme Court has traditionally interpreted the first amendment as protecting the right of the press to publish—or refrain from publishing—otherwise constitutionally protected material. See *Miami Herald Co.* v. *Tornillo,* 418 U.S. 241 (1974). News disseminators rely on First Amendment protections to publish or broadcast any information they are able to obtain. Online service providers are entitled to the same level of protection.

As modes of communication have advanced, the Supreme Court has extended increasingly broad First Amendment protections. In the online world, which is not limited to just a few speakers or a finite amount of spectrum, a vibrant marketplace of ideas will flourish without government intrusion. At this critical juncture in communications for America and for the world, we must be mindful of the risk of self-censorship; of deterring speakers and limiting the national and international debate to only those statements that are clearly acceptable to the social mainstream. As the Supreme Court cautioned in its landmark decision *New York Times* v. *Sullivan,* 376 U.S. 254, 279 (1964), such a limitation on speech "dampens the vigor and limits the variety of public debate . . . [and] is consistent with the First Amendment."

The Supreme Court explicitly recognized this principle when it recently distinguished the speech protections for cable television operators from those for broadcast television because "cable television does not suffer from the inherent limitations that characterize the broadcast medium . . . [S]oon there may be no practical limitation on the number of speakers who may use the cable medium." *Turner Broadcasting System, Inc.* v. *F.C.C.,* 114 S. Ct. 2445, 2457 (1994). Therefore, cable operators have a constitutionally protected right to select the programming they choose to carry over their systems. Id. Online service providers similarly have the constitutional right to communicate messages on a wide variety of topics through their selection of the topics of the bulletin boards and conferences they will make available to subscribers.

The legal trend has adapted Supreme Court precedent for other communications media and accorded online service providers First Amendment protections similar to those for news distributors. A federal court held that in making available a publication over which it had no editorial control, an online computer network was performing "electronic, for-profit library" functions that were entitled the same First Amendment protections accorded to distributors of publications. See *Cubby, Inc.* v. *CompuServe, Inc.,* 776 F. Supp. 135, (S.D.N.Y. 1991). Another court found that the relationship between the subscriber and the online service provider "is the same as between any subscriber and a news service; it is functionally identical to that of a purchaser of a newspaper." *Daniel* v. *Dow Jones & Co.,* 137 Misc. 2d 94, 98 (N.Y. Civ. Ct. 1987). Likewise, a court has held that, in using a person's likeness to advertise a computer bulletin board established to debate the political candidacy of the person, online computer networks should be afforded the same First Amendment

protections as newspapers, magazines, and other news disseminators. See *Stern* v. *Delphi Internet Services Corp.*, No. 122213/94 (N.Y. Sup. Ct. April 20, 1995).

In short, the First Amendment protects speech on an electronic service to no less an extent than any other publishing or dissemination activity.

Responsibilities to protect subscriber privacy rights

It also is clear that online computer networks, like telephone companies and postal authorities, cannot monitor the content of subscribers' private communications. While the general principles can be found in the Fourth Amendment, as set out in *Berger* v. *New York,* 388 U.S. 41 (1967), and *Katz* v. *United States,* 389 U.S. 347 (1967), the specific rights and responsibilities in the context of e-mail can be found in the Electronic Communications Privacy Act of 1986 ("ECPA").

18 U.S.C. §2701, enacted as part of ECPA, guarantees subscriber privacy by, among other things, prohibiting an online service provider from accessing electronically stored mail. Exceptions to the general ECPA prohibition exist for conduct authorized by the service provider, by either party to the communication, or by statutes for law enforcement purposes. None of these exceptions authorize a service provider to screen all of its subscriber e-mail.

The exception that has generated the most controversy is subsection 2701(c)(1), which directs that the prohibition against accessing stored e-mail "does not apply with respect to conduct authorized by the person or entity providing a wire or electronic communications service." The courts instruct that statutory exceptions are to be read narrowly. In the context of the statute as a whole, it is evident that this exception is intended to allow service providers the ability to authorize other entities to perform any function contemplated by the statute. The outer boundaries of acceptable conduct that a service provider can authorize are set out in sections 2701 and 2511. They do not empower a service provider to authorize a third party to conduct itself outside the law; a service provider may merely authorize another to perform billing functions or the type of service monitoring contemplated by the statute.

The courts also instruct that one should avoid interpreting one statutory provision in a way inconsistent with the policy of another provision or in a manner that would produce absurd results. If section 2701 were to be read as permitting service providers to authorize themselves to monitor the content of e-mail messages, it would be inconsistent with section 2702, which prohibits service providers from disclosing the contents of such messages. If the service provider learned of criminal activity by means of its intentional monitoring, it would be unable to report that activity pursuant to section 2702, which requires that discovery of criminal activity be "inadvertent." Thus, an open-ended reading of section 2701 would make no sense.

Moreover, the lesson from section 2702 is that the section 2701(c)(1) exception, in mirroring the corresponding exception from 2702, is intended to allow service providers the ability to authorize other entities to perform only those functions that are contemplated by the statute and necessary for the efficient operation of the communications system. Section 2702 contemplates conduct that is "necessarily incident" to the rendition of the service, such as billing and maintenance, or to the protection of the service provider's rights or property, such as anti-fraud measures. It does not sanction circumvention of the statutory proscriptions or the systematic monitoring of stored communications for evidence of a crime.[3] Likewise, the section 2701(c)(1) exception cannot be read to sanction systematic monitoring of the content of e-mail messages.

Reading section 2701 as permitting service providers to authorize themselves to monitor the content of e-mail messages also would be inconsistent with the approach taken in subsection 2703(c), which authorizes providers of electronic communications services to disclose transactional information (but not the content of communications) to nongovernmental entities. There the statute expressly authorizes providers of electronic communications services to engage in conduct less threatening to privacy than the wholesale monitoring of e-mail messages. Given the extreme nature of the intrusion contemplated by the wholesale monitoring of e-mail messages, it is dangerous to assume that the Congress would simply grant service providers the absolute right to allow any third party unfettered access to private, stored electronic communications without authorization or procedures or protections.

---

[3] For example, the House Committee Report, in discussing an exception to section 2702, states: "The sixth exception authorizes the divulgence to a law enforcement agency if the contents of the communication were inadvertently obtained and appear to pertain to the commission of a crime. This exception is intended to be read narrowly. A systematic practice of reviewing stored communications to look for evidence of a crime could not qualify as inadvertent." H.R. Rep. No. 647, 99th Cong., 2nd Sess. 67 (1986).

There is no evidence that the single phrase of subsection 2701(c)(1) was intended to eclipse the entire purpose of the ECPA.

The most harmonious reading of the section 2701(c)(1) exception restricts the conduct of service providers and authorized third parties to that which is acceptable under ECPA in its entirety. This is consistent with the traditional mode of construing a statute: in doing so, one considers the statute as a whole rather than confining oneself to the one portion at issue. It also is consistent with a careful analysis of the text, structure, and intent of the statute as embodied in all relevant sections and in the legislative history.

The result of this reading also is consistent with the responsibilities and liabilities of other providers of communications services. For example, neither the Postal Service, Federal Express, nor Bell Atlantic is expected to know the contents of handwritten mail or of telephone conversations between persons conspiring in a criminal enterprise, nor are they held liable for failing to prevent any harm that may result. Likewise, ECPA reflects that users of e-mail shall have privacy protections similar to those afforded to users of other communications services, and that computer networks are prohibited from monitoring the content of subscribers' e-mail.

CONCLUSION

Perhaps more than any other medium that has ever been used by Americans, online services support the fundamentals of our participatory democracy. Our government's role should be to facilitate—not inhibit—the development of the National and Global Information Infrastructure. And that is what government has done to date. The Congress has begun making congressional information available online; the White House and some federal agencies have set up sites on the world wide web; and federal agencies have established advisory committees to make recommendations on policies for the NII.

If America's values teach us anything, it is that particularly at times like these what we need to foster is more speech, not less.

APPENDIX A—CHILD SAFETY ON THE INFORMATION HIGHWAY [1]

A BROCHURE FOR PARENTS AND THEIR CHILDREN

Whatever it's called, millions of people are now connecting their personal computers to telephone lines so that they can "go online." Traditionally, online services have been oriented towards adults, but that's changing. An increasing number of schools are going online and, in many homes, children are logging on to commercial services, private bulletin boards, and the Internet. As a parent you need to understand the nature of these systems.

Online services are maintained by commercial, self-regulated businesses that may screen or provide editorial/user controls, when possible, of the material contained on their systems.

Computer Bulletin Boards, called BBS systems, can be operated by individuals, businesses, or organizations. The material presented is usually theme oriented offering information on hobbies and interests. While there are BBS systems that feature "adult" oriented material, most attempt to limit minors from accessing the information contained in those systems.

The Internet, a global "network of networks," is not governed by any entity. This leaves no limits or checks on the kind of information that is maintained by and accessible to Internet users.

The benefits of the information highway

The vast array of services that you currently find online is constantly growing. Reference information such as news, weather, sports, stock quotes, movie reviews, encyclopedias, and airline fares are readily available online. Users can conduct transactions such as trading stocks, making travel reservations, banking, and shop-

[1] Child Safety on the Information Highway was jointly produced by the National Center for Missing and Exploited Children (2101 Wilson Boulevard, Suite 550, Arlington, Virginia 22201–3052) and the Interactive Services Association (8403 Colesville Road, Suite 865, Silver Spring, MD 20910). This brochure was written by Lawrence J. Magid, a syndicated columnist for the Los Angeles Times, who is author of Cruising Online: Larry Magid's Guide to the New Digital Highway (Random House, 1994) and The Little PC Book (Peachpit Press, 1993).

This brochure was made possible by the generous sponsorship of: America Online, CompuServe, Delphi Internet, e-World, GEnie, Interchange Online Network, and Prodigy Services Company.

ping online. Millions of people communicate through electronic mail (E-mail) with family and friends around the world and others use the public message boards to make new friends who share common interests. As an educational and entertainment tool users can learn about virtually any topic, take a college course, or play an endless number of computer games with other users or against the computer itself. User "computing" is enhanced by accessing online thousands of shareware and free public domain software titles.*ERR0D*

Most people who use online services have mainly positive experiences. But, like any endeavor—traveling, cooking, or attending school—there are some risks. The online world, like the rest of society, is made up of a wide array of people. Most are decent and respectful, but some may be rude, obnoxious, insulting, or even mean and exploitative.

Children and teenagers get a lot of benefit from being online, but they can also be targets of crime and exploitation in this as in any other environment. Trusting, curious, and anxious to explore this new world and the relationships it brings, children and teenagers need parental supervision and common sense advice on how to be sure that their experiences in "cyberspace" are happy, healthy, and productive.

Putting the issue in perspective

Although there have been some highly-publicized cases of abuse involving computers, reported cases are relatively infrequent. Of course, like most crimes against children, many cases go unreported, expecially if the child is engaged in an activity that he or she does not want to discuss with a parent. The fact that crimes are being committed online, however, is not a reason to avoid using these services. To tell children to stop using these services would be like telling them to forgo attending college because students are sometimes victimized on campus. A better strategy would be for children to learn how to be "street smart" in order to better safeguard themselves in any potentially dangerous situation.

What are the risks?

There are a few risks for children who use online services. Teenagers are particularly at risk because they often use the computer unsupervised and because they are more likely than younger children to participate in online discussions regarding companionship, relationships, or sexual activity. Some risks are:

Exposure to inappropriate material.—One risk is that a child may be exposed to inappropriate material of a sexual or violent nature.

Physical molestation.—Another risk is that, while online, a child might provide information or arrange an encounter that could risk his or her safety or the safety of other family members. In a few cases, pedophiles have used online services and bulletin boards to gain a child's confidence and then arrange a face-to-face meeting.

Harassment.—A third risk is that a child might encounter E-mail or bulletin board messages that are harassing, demeaning, or belligerent.

How parents can reduce the risks

To help restrict your child's access to discussions, forums, or bulletin boards that contain inappropriate material, whether textual or graphic, many of the commercial online services and some private bulletin boards have systems in place for parents to block out parts of the service they feel are inappropriate for their children. If you are concerned, you should contact the service via telephone or E-mail to find out how you can add these restrictions to any accounts that your children can access.

The Internet and some private bulletin boards contain areas designed specifically for adults who wish to post, view, or read sexually explicit material. Most private bulletin board operators who post such material limit access only to people who attest that they are adults but, like any other safeguards, be aware that there are always going to be cases where adults fail to enforce them or children find ways around them.

The best way to assure that your children are having positive online experiences is to stay in touch with what they are doing. One way to do this is to spend time with your children while they're online. Have them show you what they do and ask them to teach you how to access the services.

While children and teenagers need a certain amount of privacy, they also need parental involvement and supervision in their daily lives. The same general parenting skills that apply to the "real world," also apply while online.

If you have cause for concern about your children's online activities, talk to them. Also seek out the advice and counsel of other computer users in your area and become familiar with literature on these systems. Open communication with your children, utilization of such computer resources, and getting online yourself will help

36-038 O - 97 - 3

you obtain the full benefits of these systems and alert you to any potential problem that may occur with their use.

Guidelines for parents

By taking responsibility for your children's online computer use, parents can greatly minimize any potential risks of being online. Make it a family rule to:

Never give out identifying information—home address, school name, or telephone number—in a public message such as chat or bulletin boards, and be sure you're dealing with someone that both you and your child know and trust before giving it out via E-mail. Think carefully before revealing any personal information such as age, marital status, or financial information. Consider using a pseudonym or unlisting your child's name if your service allows it.

Get to know the services your child uses. If you don't know how to log on, get your child to show you. Find out what types of information it offers and whether there are ways for parents to block out objectionable material.

Never allow a child to arrange a face-to-face meeting with another computer user without parental permission. If a meeting is arranged, make the first one in a public spot, and be sure to accompany your child.

Never respond to messages or bulletin board items that are suggestive, obscene, belligerent, threatening, or make you feel uncomfortable. Encourage your children to tell you if they encounter such messages. If you or your child receives a message that is harassing, or of a sexual nature, or threatening, forward a copy of the message to your service provider and ask for their assistance. Should you become aware of the transmission, use, or viewing of child pornography while online, immediately report this to the National Center for Missing and Exploited Children by calling 1–800–843–5678. You should also notify your online service.

Remember that people online may not be who they seem. Because you can't see or even hear the person it would be easy for someone to misrepresent him- or herself. Thus, someone indicating that "she" is a "12-year-old girl" could in reality be a 40-year-old man.

Remember that everything you read online may not be true. Any offer that's "too good to be true" probably is. Be very careful about any offers that involve your coming to a meeting or having someone visit your house.

Set reasonable rules and guidelines for computer use by your children (see "My Rules for Online Safety" on last page as sample). Discuss these rules and post them near the computer as a reminder. Remember to monitor their compliance with these rules, especially when it comes to the amount of time your children spend on the computer. A child or teenager's excessive use of online services or bulletin boards, especially late at night, may be a clue that there is a potential problem. Remember that personal computers and online services should not be used as electronic babysitters.

Be sure to make this a family activity. Consider keeping the computer in a family room rather than the child's bedroom. Get to know their "online friends" just as you get to know all of their other friends.

My rules for Online safety

I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.

I will tell my parents right away if I come across any information that makes me feel uncomfortable.

I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.

I will never send a person my picture or anything else without first checking with my parents.

I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the online service.

I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.

For further information on child safety or a free copy of the brochure, please call the National Center for Missing and Exploited Children at 1–800–THE–LOST (1–800–843–5678).

Appendix B—Membership List

1–800 Flowers/800–GIFTHOUSE, 101 Online, Accu-Weather Inc., Accurate Info Ltd., Acxiom, Advanced Telecom Services, Aegis Publishing Group, AGT Directory Limited, Air One Inc., Aircraft Owners & Pilots Association, Allstate Communications, America Online, Inc., American Airlines/EAASY SABRE, American Express, American Greetings, American Telnet, Ameritech Development Corporation, Apple Online Services, Arlen Communications, Inc., Associated Press Information Services, AT&T, Audiotex Directory, Audiotex News, Inc., Aural Digital Conference Marketing (ADCM), Bank of America, Bank South, Barrels of Fun, Bellcore, BFD Productions, Inc., Bloomberg Business News, BTT, Budd, Lamer, Gross, Rosenbaum, Greenberg & Sade, Bureau One Inc.

Cable TV Administration & Marketing Society, Inc., Cabot, Richards & Reed, Call Interactive, CANNEX Financial Exchanges Limited, Capital Gains Inc., Cavanagh Associates, Inc., CD3 Consulting, Inc., Cetesa, Chase Manhattan Bank, NA, Checkfree Corporation, Citibank, N.A., City of Hampton, Cole Group, Columbia Tristar Television, Columbia University, The Freedom Forum, CommSys Corp., CompuServe Incorporated, Concentric Research Corporation, Conhaim Associates, Inc., Consumers Union, Continental Cablevision, Inc., Corporate Television Network, CUC International, CyberMark, Inc., Dalton Associates, Damark International Inc., Data Times, Delphi Internet Services, Deutsche Telekom, Dickstein, Shapiro & Morin, Digital Information Group, Direct American Marketers, DirectLink Technologies Corp., DirectoryNet, Inc., Don Allan Associates of nj, Inc.

Dunnington, Bartholow & Miller, EchoVision, Inc., EDS—Electronic Commerce Division, EDS Management Consulting Services, Education On-Line, EDventure Holdings, Inc., Electronic Messaging Association, Enterprise Communications—Infotext, Entertainment Connection, Inc., EON Corporation, Etak, Inc., Everett Multimedia & Design, FBN Software, Inc., Find/SVP, Fingerhut Corporation, First Data Corporation, First Telecom/First Tennessee, Fonawin, Inc., Ford Motor Company, Forrester Research, FTD Direct Access, Inc., Fujitsu Cultural Technologies, Future Freedom, Future Systems Incorporated, Gary D. Schulz.

Gateway Software, Inc., General Electric, General Media Worldwide Online Services, Inc., George Kois, GeoWorks, Ginsburg, Feldman & Bress, GRAFF Pay-Per-View, GRAFX Group, Inc., Grey Advertising, GTE Main Street, Hall, Dickler, Kent, Friedman & Wood, Hallmark Cards, Inc., Hawaii INC, Heartland Free-net Incorporated, Heritage Newspapers, Hewlett Packard, Home Box Office (HBO), Honeywell, Inc., Hong Kong Telecom CSL, HSN Interactive, Hughes New Venture Organization, ICN Corporation, IdealDial, Image Base Videotex Design, IMATEX Communications, Inc., Info Access Inc., Information & Interactive Services Report, Institute For the Future, Intel Corporation, Intellimedia Sports Inc., Interactive Development Corporation, Interactive Marketing Group Inc., Interactive Marketing Inc., Interactive Media Associates, Interactive Media, Inc., Interactive Media Works, Interactive Multimedia Association, Interactive Network, Interactive Publishing, Interactive Telecommunications Services, Interactive Transaction Partners ITP, Interactive Video Enterprises, Inc., Interaxx Television Network, Inc., International Telemedia Association Inc.

Interval Research Corporation, Intuit, ISED Corporation, Issue Dynamics, IT Network, Inc., ITT World Directories, IVI Publishing, Inc., J. Walter Thompson, Jared, The Galleria of Jewlery, JCC Technologies, Inc., John Hall & Company, Jupiter Communications, Ketchum Interactive Group, Landmark Communications, Lands' End, Lapin East-West, Lincoln Telephone & Telegraph Co., LINK Resources Corporation, Litle & Company, Lo/Ad Communications, Lochridge & Company, Long Distance Billing Company, Inc., Los Angeles Times, Loto Quebec, MarCole Enterprises, Inc., Maritz, Inc., Market Information Exchange (MIX), Marketing & Advertising Services Center, Inc., Marketing Corporation of America, Martin Hensel Corporation, MasterCard International, McClatchy Newspapers, MCI Communications, MCI Telecommunications, Media General Inc., Mellon Bank, NA, Meridian Bank.

Metamark International, Metromail Corporation, Michael Wolff & Company, Inc., Micro Voice Applications Inc., Microsoft, Midlun HF, Midratel US Inc., Moore Telecommunications, Morris Information Services, MultiComm Development, National Telephone Enterprises, Network Telephone Services, Neue Mediengesellschaft Ulm mbH, New Tech Telemedia, New Times Inc./NTI Communications, New York Switch Corporation, New York University, Newhouse New Media, Inc., News America New Media, Newsday, NIFTY Corporation, Norpak Corporation, North American Publishing, Co., Northern Telecom, Northwest Nevada Telco, NPD Group, NUSTAR International, Inc., NYNEX Corporation, Octel Communication, Ogilvy & Mather Direct, Online Interactive, Optigon Interactive.

Pacific Telesis, PAFET, Pamet River Partners, Pandora Systems International, Parks Associates, Pat Dunbar & Associates, Pay Per Call Ventures, PC Financial Network, PC Flowers Inc., PC Travel, PeaPod, Philips, PhoCusWright, Phoenix Newspaper, Inc., (PAFET), Phone Programs, Inc., Physicians' Online, Inc., Pineapple, Ltd., Pinellas County Review, Presentation Works, Prevue Interactive Services, Prodigy Services Co., ProductView Interactive, Inc., Publications Resource Group, Pultizer Publishing, Company, Reality Online, Inc., Reuters New Media, Inc., Rio Grande Travel, RJ Gordon & Company Inc., Rosenbluth Travel/Travelmation, Saco River Tel & Tel Co., San Jose Mercury News, Sanoma Corporation, SBC Communications, Scholastic Network, Scripps Howard.

SECOM Information System Corp., Seelinger Communications, SIMBA Information Inc., Simutronics, SITEL, Skytel, SmartPhone Communications, Inc., Southam Electronic Publishing, Springboard Productions/The Workshop, Sprint Telemedia, St. Clair Interactive Communications, St. Petersburg Times, Star Tribune, Starwave Corporation, Stentor Resource Center Inc., STM Consulting Pty., Ltd., Strategic Telemedia, Sullivan Communications, Sure Find Classifieds, Swedish Information Technology Commission, Swiss Online, Symphony Management Associates, Inc., Talking Classified, (TDF) Telediffusion de France, TecNet, Telco Communications Group, Tele Denmark Ktas Publishing, Tele-Direct (Pub), Inc., Tele-Lawyer, Inc., Tele-Publishing, Inc., Telebase Systems, Telecom Finland, Telecompute Corporation, Telemedia Network, Inc., TELMO ry, The Globe & Mail, The Hotel Industry Switch Company, The Imagination Network.

The Infoworks Group, The Kelsey Group, The Marx Group, The Promus Hotel, The WELL, Times Information Services, Inc., TMA Productions, Tom Lehman & Associates, Tom Morgan, Trademark Register, TraveLOGIX, Tremblay & Company, Tribune Interactive Network Services, Tribune Media Services, TV Alphaville Sistemas de Communicao a Cabo, TV Data Technologies, U S West Communications, United Advertising Publications, Universal Teleservices Corporation, US Order, US Postal Service, USA Tax Service, USA Today—Gannett Information Services, USAA.

VeriFone, Inc., VIACOM Interactive Media, VICOM Information Service, Vicorp Interactive Systems, Inc., Videoway Communications, Inc., Virtual Arts Online Systems, Inc., Virtual Shopping, Inc., Virtual Vegas Incorporated, VISA, VISION Integrated Marketing, Visual Services, Inc., Voice FX Corporation, Voicelink Communications, Vos, Gruppo, & Capell, Inc., VRS Billing Systems Inc., Washington Post Company, Weather Concepts, Inc., Weissmann Travel Reports, West Interactive Corporation, Women's Wire, Working Assets Long Distance, Worldspan, Worldview Systems Corporation, Wundeman Cato Johnson, Ziff-Davis Interactive, Zycom Network Services, Inc.

Senator SPECTER. Thank you, Mr. Burrington.

We now turn to Mr. Jerry Berman, executive director, Center for Democracy and Technology.

STATEMENT OF JERRY BERMAN, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. BERMAN. Thank you. The Center for Democracy and Technology is a civil liberties organization concerned with achieving the democratic potential of new communications technologies. We care about the Internet, and we believe it is one of the most important democratic experiments underway today.

Yes, you can find terrorist manuals on the Internet. You can find organizations who believe that our Government is illegitimate. There are people calling for destruction of our Government, taking action against Government officials.

But, to judge the Internet solely by that is really a mischaracterization. The Internet is also Senator Leahy's Web page. It is also, if you dial up "bomb" on the Internet and ask for an index, you would get the FBI's Web page, which has information on the Unabomber and tips and their effort to investigate and they are encouraging citizens to help them in that effort.

If you dial up "terrorist," you might get not only that there is a "Star Trek" episode on terrorism, but you will also get a terrorist profile weekly where people are keeping track of terrorist organizations.

It is absolutely a wide-open network. It is consistent with the first amendment, and we need to really understand that it is the chance to achieve what we call the electronic Gutenberg, a massive public forum which gives more citizens more easy access and ability to participate in the political process to organize, to reach their Congressman, to discuss ideas. Anything that threatens that free speech, I think, is contrary to our democratic principles, and also, plays into the hands of terrorists.

The argument of the terrorists is that our society is not open, that its political processes are closed, and that you must resort to violent action in order to right wrongs. The Internet is a prime example, a living example, that this is an open society and that political debate can go on. If a speech, like the Rabbi pointed out, comes on the Internet, you can answer that speech with more speech.

Everyone testifying today has argued that in this area, when we are talking about punishing speech, we need speech plus. The Brandenburg doctrine is not just advocacy of illegal activity, but imminent lawless conduct.

When we look at the Internet, while there is a lot of vociferous speech going on—and maybe it is encouraged by the anonymity and the fact that people are sitting at their computers in different places and we have a new technology and we don't understand all of the customs, yet—our belief is that focusing on the Internet is, if you do, it is very different than Justice Holmes' warning that you can be punished for falsely shouting fire in a crowded room. The Internet is not a crowded room.

It is dispersed people, speaking from the bedroom or from their office or from their apartment, using their computer and speaking to each other.

So that, simply focusing on speech on the Internet, from a prosecutorial point of view, would be, I think, not enough. Prosecution requires more. Even the idea of someone with a terrorist manual or even organizing and saying, "Let's go surround that court building," which is the Cox case. There, you have speech plus.

Organizing people on the Internet, you still have to get off the Internet. You still have to arrive somewhere. You still have to have guns. You still have to have militia uniforms and so forth.

So, in that context, we believe that there should be far less concern about the Internet and far less focus from a prosecutorial point of view.

I want to talk about the other prong, which is, what can you investigate on the Internet? Under the FBI guidelines, the guidelines today are focused on criminal activity. There has to be a nexus between speech and violent activity or illegal activity for a political cause to intimidate and so forth.

Those guidelines have the flexibility to allow the FBI to target a militia group, if you have more than speech, or an organization that is advocating illegal activity on the Net. But the reason that we have those guidelines focused on criminal activity and not on political speech is because we went through a long period of open-

ended investigations by the FBI where they targeted 500,000 investigations with very little prevention of violence and chilling speech.

We do not want to loosen those guidelines or create the impression that the FBI is now a vacuum cleaner sweeping up information of lawful speech on the Internet.

I believe that that would be contrary to the first amendment and contrary to lawful and important law enforcement interests.

I am prepared to discuss these interests, but in closing, it is really urging caution, urging study, urging support of Senator Leahy's legislation, supported by Senator Kohl, which says, let's look at the Internet as a new free speech avenue and how we protect our children in that atmosphere without creating unwarranted criminal statutes.

I look forward to answering your questions. Thank you.

[The prepared statement of Mr. Berman follows:]

PREPARED STATEMENT OF JERRY BERMAN

Mr. Chairman and Members of the Subcommittee: My name is Jerry Berman, Executive Director of the Center for Democracy and Technology. The Center is pleased to have opportunity to address the subcommittee on one of the critical civil liberties issues of our day: the right to free speech, free association, and privacy on the Internet in the aftermath of Oklahoma City. The Center for Democracy and Technology is an independent, non-profit public interest policy organization in Washington, DC. The Center's mission is to develop and implement public policies to protect and advance individual liberty and democratic values in new digital media. The Center achieves its goals through policy development, public education, and coalition building.

I. OVERVIEW: SHOUTING FIRE IN CYBERSPACE—FIRST AMENDMENT IMPLICATIONS

The recent tragedy of Oklahoma City brings us here with questions and concerns about terrorist activity and constitutional rights on the Internet. The Internet is a global network of networks that connects over twenty million users around the world. Each day hundreds of thousands of documents and millions of electronic mail messages are exchanged through these interconnected computers.

Yes, there is information on the Internet about how to build bombs, reasons to overthrow the United States Government, and how to organize violent militia groups. The question facing us, as an open society, is how to respond to the most controversial and extreme uses of this new technology, this electronic global Gutenberg printing press that turns all citizens into publishers who can reach thousands and even millions of people around the country and the world.

As an open society, governed by the democratic principles of the First and Fourth Amendments, we tolerate and even encourage robust debate, advocacy and exchange of information on all subjects and in all media of expression, without exception. Prior restraint or any government action which might chill speech have long been labeled intolerable, except in the few circumstances in which that speech advocates imminent violence and is likely to produce such violence. Even in these cases, Constitutional law and longstanding law enforcement policy have dictated great restraint in order to avoid chilling legitimate speech activity.

Justice Holmes taught that the First Amendment does not protect a person from punishment for "falsely shouting fire in a theater and causing a panic," *Schenk* v. *United States,* 249 U.S. 47, 52 (1919), but what does it mean to "shout fire" in cyberspace? We believe that shouting fire in cyberspace is actually *far less threatening,* and thus less deserving of censure, than the equivalent act in the physical world. Though one can shout fire in an email message or on an Internet newsgroup, the likelihood that it will incite readers to imminent, criminal action is much reduced because the readers are dispersed around the country, and even around the world.

As interactive media such as the Internet become more and more common in public life, we will be challenged to revisit these basic issues about the difference between protected advocacy and truly dangerous action. Articulating this line, over which government investigation and prosecution must not cross, requires faithfulness to the traditions of our open society and careful attention to the unique characteristics of this new medium. Answering these questions is particularly important

because the Internet is the site of new, vibrant political discourse and information. Given the political character of communication in online environments, it is especially important that First Amendment activity and privacy rights be protected.

Indeed, in the face of terrorist threats, it is particularly important to maintain an open society in order to minimize public paranoia about the government and to discredit the arguments of those who advocate the destruction of our government. The openness of the Internet and other interactive media should be seen as a great boon to our democracy, not as a threat to order. A noted scholar of terrorist behavior notes that:

"The U.S. has been remarkably free of political terrorism because the U.S. institutions for conflict resolution and justice redress, available to everyone, were believed to be working by and large in a satisfactory manner." [1]

Following Oklahoma City, the debate over counterterrorism policy has presupposed that the openness of our society is at odds with the fight against domestic terrorists. At least in the case of political advocacy on the Internet, we believe that a policy that promotes openness can help heal the paranoia and distrust of government and the political process by engaging the citizenry in a new political forum.

The Center for Democracy and Technology believes that any prosecutorial or investigative activity must be predicated on speech plus a reasonable indication that the speech will lead to imminent violence. Speech alone is not enough to prosecute or investigate in other media, and it should not be sufficient in interactive media. Moreover, we assert that current law and the FBI's strict interpretation of the existing Attorney General investigative guidelines are adequate to serve both law enforcement purposes and First Amendment interests.

II. POLITICAL DISCOURSE ON THE NET: DEMOCRACY FLOURISHING ANEW IN INTERACTIVE MEDIA

To judge the Internet solely by the aspects of this new medium that have caught Congressional attention this year would lead to the belief that it is a haven for bomb-makers, militia members, racists, and purveyors of child pornography. Yet this view of the Internet fails to account for the great democratic potential of interactive media, and the fact that a considerable degree of political discussion, grass roots organizing, and political education takes place on the Internet today. Indeed, if present usage patterns continue, we believe that the Internet has the potential to revitalize political discourse by providing citizens with access to more detailed information about the political process and by creating a forum for political organizing that includes far more citizens in the political process than does the passive politics of television-based campaigning.[2] This potential will be chilled if the medium is not properly protected from intrusion.

As the popularity and accessibility of the Internet and commercial online services grows, and as the medium becomes easier to use, the political uses of the net are flourishing. Political discourse is facilitated by a variety of different communications techniques available online, including newsgroups, mailing list discussion groups, chat sessions, and a host of electronic publishing capabilities.

Newsgroups: News groups are open, public areas in which users "post" articles and comments on a variety of subjects. Unsenet newsgroups accessible around the world on the internet may be thought of as a hybrid of a newspaper, because of their broad reach, and community bulletin boards, because of their interactivity and ease of access. Each newsgroup is devoted to a particular subject, from discussion of abortion, privacy rights, to the views of President Clinton and Rush Limbaugh. Newsgroups are read by thousands or even millions of people, and any one who reads the group can also contribute to the discussion by posting his or her own comments. [See Appendix B for a list of politically-oriented newsgroups]

Public mailing lists: Those who have an interest in exchanging information about a particular subject may also join a public mailing list on that subject. Mailing lists enable all members to exchange electronic mail messages easily and allow others to join their discussions. Unlike newsgroups, many mailing lists that are open to the public enable participants to obtain a list of those who are participating in the discussion.

Private mailing lists: In some circumstances, an existing group of people will create a private mailing list to enable the group to discuss issues in private through the exchange of electronic mail. These lists are considered closed to the public and the identity of each participant is generally known.

---

[1] F. Hacker, "Crusaders, Criminals, Crazies: Terror and Terrorism in Our Time," 67 (1976).

[2] See Berman & Weitzner, "Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media," 104 Yale.L.J. 1619 (1995).

Interactive chat services: A variety of services are available to enable a group of people to engage in live, instantaneous communications. These services might be characterized as conference calls, social gatherings, or town meetings in cyberspace. As with mailing lists, the chat sessions may be either public or private. The name or identity of each participant is generally known.

These services have been used to hold public conferences and discussion sessions on a variety of subjects from music to politics. A geographically dispersed political group might well use interactive chat services to hold a meeting online.

Electronic publishing: The Internet is a revolutionary medium for delivering and receiving information inasmuch as distribution is rapid at a low cost compared to print publication. Services such as the World Wide Web enable any individual or organization to quickly disseminate documents, images and even video to individuals all over the world.

The Center for Democracy and Technology has found World Wide Web services critical to our own public education activities, and an increasing number of grass roots and community groups are coming to rely on the internet to keep in touch with members and constituents. In fact, even some Senators offices are using the World Wide Web to communicate with and solicit feedback from constituents.[3] [See appendix A for a list of politically-oriented World Wide Web sites.]

Political groups left, right, and center are using the internet to communicate, to organize, and to advocate their own views. As a nation we should be encouraging political discourse in this new medium, because of its potential to raise the level of political discussion beyond the soundbite and to involve more citizens in the political process. One aspect of encouraging political discourse in interactive media is to assure all users that their First Amendment and privacy rights will be respected fully.

III. LIMITS ON LAW ENFORCEMENT ACTIVITY IN PURE SPEECH ENVIRONMENTS SUCH AS THE INTERNET

All discussions and exchanges of information on the Internet are speech, and thus any proposal to criminalize or investigate such activity triggers a heightened degree of scrutiny. The tradition of prosecutional and investigative sensitivity in areas involving First Amendment activity is both long standing and well-founded in our democratic traditions. We outline here the restrictions that have traditionally safeguarded political activity from harmful, chilling government interference, and suggest ways in which their application to cyberspace poses unique, new questions.

In our preparation for this hearing, we have found information on how to construct bombs on the Internet. Curiously, the most detailed information that we found comes from Internet sites located outside the United States. The Terrorist Handbook, that contains information on how to make bombs similar to the one used in Oklahoma City, is available from a British World Wide Web site.[4] And, information on how to make an atomic bomb can be found on a Swedish site.[5]

A. Heightened standard for prosecution of crimes involving first amendment rights

Even putting the problems of international criminal jurisdiction aside, we believe that the mere publication of these bomb manuals is protected by the First Amendment from criminal sanction. Criminal prosecution of speech-related activity must withstand the two-pronged test established by the Supreme Court in *Brandenberg* v. *Ohio,* 395 U.S. 444 (1969). Advocacy may not be proscribed unless it (1) "is directed to inciting or producing imminent lawless action," and (2) that such advocacy is "likely to . . . produce such action." Id. at 447. Both the call to immediate criminal action and the likelihood that such a call will be heeded are necessary to justify prosecution. Advocacy of violence alone is insufficient. *Yates* v. *United States,* 354 U.S. 298, 318 (1957), (advocacy and teaching forcible overthrow of the government is immune from prosecution under the First Amendment). Taken together, these cases form what is commonly referred to as the "speech plus" doctrine. Some action or evidence of action beyond mere words must exist to justify a criminal prosecution of political advocacy activity. *Cox* v. *Louisiana,* 379 U.S. 559, 563 (1965). In *Cox,* the "plus" that justified prosecution of the advocacy in the course of a street demonstration was the imminent threat that the demonstrators would violently attack the county courthouse around which they were circling.

Speech and advocacy on the Internet, unlike a street demonstration, are pure speech, with no immediate threat of physical violence, in all of the circumstances

---

[3] See Senator Patrick Leahy's World Wide Web site at ftp://ftp.senate.gov/member/vt/leahy/general/pjl.html.

[4] This document can be found at the following URL—http://www.mcs.dundee.ac.uk:8080/-apaterso/terror.txt.

[5] See URLhttp://www.nada.kth.se/-nv91-asa/atomic.html.

that we can imagine. As passionate and vehement as speech on the Internet may be, it remains only speech, with no immediate nexus to violence in most situations. Unlike the crowded street in which demonstrators circle a building, no matter how incendiary the words sent over the Internet may be, they are still a long way from causing criminal harm. Words sent over the Internet may inspire or incite, but the nexus between the words and subsequent action is far more attenuated than any case in which the Court has approved criminal sanction. Thus, we believe that even if one publishes bomb-making instructions online, the second prong of *Brandenberg* is not satisfied. There is no "plus" incident to the publication of a document that constitutes action likely to produce violence.[6]

B. Tradition of special status for law enforcement investigations involving political groups and exercise of first amendment rights

Further recognition of the sensitivity of law enforcement intrusion on First Amendment activities is found in the Attorney General's Guidelines governing investigation, infiltrations, and information collection involving First Amendment activities. In response to several decades of law enforcement harassment of political organizations, these guidelines establish the general principle that law enforcement may not interfere with political activity based solely on predicates drawn from the speech and advocacy activities of political groups. As in the prosecutorial standard described above, something more than speech is required before investigations, infiltrations, or intrusive infiltration gathering activities are commenced.

1. Speech plus required to open an investigation

The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigation[7] are in place in order to "encourage Agents of the FBI to perform their duties with greater certainty, confidence and effectiveness," and to "give the public firm assurance that the FBI is acting properly under the law." This dual purpose guides the FBI toward the most effective investigative path, and assures the public that their free speech and privacy rights are fully respected. Of particular relevance to this hearing are the guidelines as they relate to domestic security/terrorism investigations. The guidelines state: "A domestic security/terrorism investigation may be initiated when the facts or circumstances reasonably indicate that two or more persons are engaged in an enterprise for the purpose of furthering political or social goals wholly or in part through activities that involve force or violence and a violation of the criminal laws of the United States." p. 13.

These guidelines describe requirements for opening full investigations, and also, procedures and requirements for opening preliminary inquiries, which include investigative activity where a full investigation is not necessary or not yet justified.

The Investigation Guidelines recognize all political activity as "sensitive" to undue law enforcement intrusion. Two provisions exists to safeguard sensitive First Amendment activity from the chilling effect of improper intrusion.

Speech plus predicate for a full investigation: The Investigative Guidelines clearly state that a full investigation may not be commenced based "solely on activities protected by the First Amendment or on the lawful exercise of any other rights secured by the Constitution" if there is no "prospect of harm." p. 3.

Supervisory approval required for intrusion on political matters: In the event that a full investigation or even merely a preliminary inquire is to be opened involving "sensitive" matters, including the investigation of political groups, supervisory approval is required before proceeding. p. 4–5.

Given this tradition of forbearance in the case of investigations of First Amendment-protected activity, we would expect that all investigations and preliminary in-

---

[6] The publication of a bomb-making manual on the Internet is factually distinct from the publication of instructions on making a hydrogen bomb that was injoined in *United States* v. *Progressive, Inc.*, 467 F.Supp 990 (W.D. Wisc. 1979). In that case, the material which was enjoined was classified and was held no dangerous that it could lead to world-wide conflagration. *Id.* at 995. The article was ultimately published and the case became moot because the information previously held as classified was found in a number of public libraries.

We would also distinguish *Near* v. *Minnesota*, 283 U.S. 697 (1931), a case approving the bar of publication of troop movements in local newspapers. *Near* stakes out an extremely narrow area involving prior restraint for the sake of national security threats, such as the location of troops. The threat of bomb-making information—all of which is generally available in libraries, chemical text books, and farming manuals—is clearly not as great as the disclosure of military strategy.

[7] Guidelines originally issued by Attorney General Edward Levi in 1976 and modified by William French Smith in 1983 and Richard Thornburg in 1989. Hereinafter Investigation Guidelines.

quiries involving political activity on the Internet or other interactive media would be subject to the above requirements.

2. Limitations on infiltrations

Historically, law enforcement infiltration of domestic political groups has been shown to be excessive and violative of individual's right to free association. The Attorney General's Guidelines on FBI Use of Information and Confidential Sources[8] were issued in order to set reasonable limits on law enforcement's use of these techniques. Like the Investigative Guidelines, the Infiltration Guidelines also recognize that extra care is needed when the use of these techniques implications First Amendment activities. In assessing the appropriateness of a particular operation, the FBI must consider the risk of intrusion upon "lawful association of individuals or expression of ideas." p. 3, 11. As with the Investigative Guidelines, supervisory approval is required for the use of an informant or confidential source who will "make use of formal or informal affiliation with an organization that is predominantly engaged in political activities." p. 11. Furthermore, the FBI intrusion must be assessed in light of its potential to "hinder the ability of the organization to function." p. 11.

Inasmuch as many of the political activities undertaken in interactive media involve group discussion and planning, concerns raised by the Guidelines are especially relevant to any law enforcement activity online. We believe that this new medium raised many questions as to the proper role of law enforcement in light of these Guidelines. For example:

Can law enforcement agents participate in online discussion groups?

We believe that it may be allowed under the guidelines for law enforcement agents to read Usenet newsgroups under certain circumstances, however we are gravely concerned that the Bureau should not train a large vacuum cleaner on the Internet for the purpose of collecting masses of information as to the political views of individual citizens, especially where those citizens are in no nexus to any criminal activity.

If so, must they announce their identity as law enforcement officers to the group? If not, must they disclose their identity if asked?

Absent authorization for infiltration under the Justice Department's criminal investigation standard, we believe that law enforcement agents should certainly be required to identify themselves.

C. First and fourth amendment nexus: protecting privacy rights to ensure first amendment rights

To encourage full political participation by all citizens requires that law enforcement respect individual privacy, as well as free speech rights. For, if individuals feel that they may be investigated, tracked, or otherwise subject to government scrutiny merely or association with a particular political idea or group, then they may be less likely to vigorously participate in the political process. The Court has long recognized the nexus between the First Amendment and Fourth Amendment privacy rights. *United States* v. *United States District Court,* 407 U.S. 297 (1972) (warrantless wiretap not only violates Fourth Amendment, but also implicates the First Amendment). Recognizing these concerns, the various Attorney General guidelines discussed above, as well as the Privacy Act, puts limits on the degree to which law enforcement may invade the privacy of individual and group political activity.

In the absence of an authorized FBI inquiry or investigation, the Bureau is barred from maintaining any record on the First Amendment-protected activities of individuals. Section (e)(7) of the Privacy Act of 1974 (5 U.S.C. 552a) provides that: "Each agency that maintans a system of records shall maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about who the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."

Congress included Subsection (e)(7) in the Act to reassure the American public that the FBI, CIA and the military would no longer have free reign to monitor and maintain files on the first amendment-protected activities of citizens. The Senate Report on the bill explains that "[t]his section's restraint is aimed particularly at preventing collection of protected information, not immediately needed, about law-abiding Americans, on the off-chance that Government or the particular agency might possibly have to deal with them in the future." (S. Rept. 93–1183) As Representative Abner Mikva pointed out in hearings leading up to the passage of the Privacy Act: "The harm comes when the ordinary citizen feels he cannot engage in

[8] Issued in 1980 by Attorney General Benjamin Civilette.

political activity without becoming a 'person of interest,' without having his name and photo placed in a file colloquially, if not officially, labeled 'subversive.'"

In floor debate on the final wording of the section, the importance of protecting lawful speech was underscored: "[N]o records or files shall be kept on persons which are not within constitutional limitations. . The rights of Americans to dissent in a lawful manner and for lawful purposes must be preserved."

In guidance issued by the Office of Management and Budget in December, 1975, the (e)(7) prohibition was interpreted to bar the collection of information on individuals even if the information was published and considered publicly available, with the exception of standard bibliographic or library reference materials: "Collections of newspaper clippings or other published matter about an individual maintained other than in a conventional reference library would normally be a system of records [and thus subject to the Privacy Act]."

Further, a 1983 Justice Department memorandum intended to clarify the Privacy Act application to FBI collection of publicly available information concluded: "that unless the individual or group meets the standard for either a preliminary inquiry or a domestic security/terrorism investigation, collection of published materials, outside the library context, is barred." It is important to note, however, that the FBI guidelines state in the General Principles section that "Nothing in these guidelines is intended to prohibit the FBI from collecting and maintaining publicly available information consistent with the Privacy Act."

An issue here is how the (e)(7) prohibition applies along the continuum of speech activities on the Internet. Both the Privacy Act and the FBI guidelines were written before the development of the Internet. A question exists as to whether, for instance, newsgroup communications are to be publicly available information for purposes of collection by the FBI.

IV. RECOMMENDATIONS

In conclusion, we want to commend Chairman Specter and this subcommittee for your diligence in addressing this very important issue. We close with the following recommendations:

- *Don't criminalize pure speech:* Our First Amendment traditions and longstanding law enforcement policy teach that criminal sanctions are only appropriate for "speech plus" some criminal or likely violent action.
- *Maintain cautious interpretation of Attorney General's guidelines in online investigations:* Cautious interpretations of the current guidelines leave the FBI plenty of room to investigate genuine threats and provide the citizenry reassurance that their political activities, even where controversial, are not subject to government scrutiny and intrusion.
- *Start of dialogue on the proper role of law enforcement in policing the online world:* We hope that this hearing is the first step in a process that establishes, based on a broad public dialogue, how law enforcement can be expected to function in the new online environment.

One venue for such a dialogue is the legislation (S. 714) that Senator Leahy has introduced, calling for a study of proper legal responses to violence, hate speech, and sexually-explicit material in interactive media. We commend Senator Leahy for his leadership on this issue, and are grateful to Senator Kohl for his co-sponsorship of the Leahy study. We have also been in discussions with this subcommittee about the study, and look forward to working with you.

- *Treat proposals to expand surveillance authority with great caution:* In the wake of the Oklahoma City tragedy, law enforcement and the Administration are proposing dramatic changes to federal wiretap authority including new roving tap powers and the use of any federal criminal statute as the predicate for wiretaps in terrorism investigations. Just last year, the Congress enacted changes to wiretap law in the Digital Telephony bill. The changes now sought were not raised in the context of last year's bill and there is no indication that any of the changes sought this year are justified by new circumstances.

Though these issues are beyond the scope of today's hearing, we do want to note for the record that we are very concerned about expansion in roving tap authority, additions to the list of predicate crimes for electronic surveillance, as well as other records access provisions proposed in various counterterrorism bills now before both houses of Congress.

Again, we thank the Chair for the opportunity to appear before you on this very important issue and are ready and willing to work with you on these critical civil liberties issues affecting interactive media.

Appendix A—Politically Oriented World Wide Web Sites

GENERAL RESOURCE

Political participation project

http://www.ai.mit.edu/projects/pp/home.html

The Political Participation Project is a research program investigating how computer networks can be used to facilitate political participation. The Project's mission is to design networked, interactive media that improve citizens' participation in the democratic process. The Project, affiliated with the Intelligent Information Infrastructure Project at MIT, is non-profit and non-partisan.

Project Vote Smart

http://www.peak.org/~votesmrt/

Project Vote Smart is a voter's self-defense system that provides the voter with factual information on candidates and elected officials.

Interactive Democracy

http://www.teleport.com/~pcllgn/id.html

A free service that provides a gateway to allow individuals to send email messages to a list of representatives of government and the media.

NewtWatch

http://www.cais.com/newtwatch/

NewtWatch is a new web service designed to be your resource on Speaker of the House Newt Gingrich. Contains information on Gingrich's voting records, political contributions, legislative efforts, and more.

Clinton Watch

gopher://dolphin.gulf.net:3000/

Clinton Watch is a political column on the Internet devoted to a critical analysis of the policies and actions of the Clinton administration.

CONSERVATIVE SITES

The Conservative Link

http://www.moscow.com/mdesign/tcl/conintro.html

The Conservative Link is a page for people who share the conservative point of view.

The Right Side of the Web

http://www.clark.net/pub/jeffd/index.html

The Right Side of the Web is a unique listing of resources for political conservatives. The page contains links to other conservative oriented sites, email lists, publications/editorials, and links to other political groups (including liberal groups).

LIBERAL SITES

The Left Side of the Web

http://paul.spu.edu/~sinnfein/progressive.html

The Left Side of the Web—Links to liberal related resources, newsgroups, publications, and file archives

Progressive Page

http://www.io.org/~spamily/SocPolEnv.html

A collection of links for progressives, feminists, liberals, and anyone else who's interested.

POLITICAL ORGANIZATIONS

The Center For Democracy And Technology

http://www.cdt.org/

CDT is a non profit public interest organization working to develop and advocate public policies that preserve and enhance democratic values in new communications media.

The Progress and Freedom Foundation

http://www.pff.org/

The Progress and Freedom Foundation a non-profit organization dedicated to creating a positive vision of the future.

Internet Headquarters for the Republican Primary

http://www.umr.edu/~sears/primary/main.html

Internet Headquarters for the Republican Primary—info on who are running, who may run, and who's not running for President in the Republican party.

Democratic Senatorial Campaign Committee

http://www.dscc.org/d/dscc.html

Over the next several months, look for new information about potential candidates, impact issues in 1996, and other DSCC activities.

United We Stand America

http://www.telusys.com/uwsa.html

An educational, nonpartisan, nonprofit organization designed to inform the public about the important issues facing our country and to give our members a voice in the way we are governed.

Rock The Vote

http://www.iuma.com/RTV/

Rock The Vote—national organization for young people based on one simple idea: young Americans deserve to be heard.

APPENDIX B—POLITICALLY ORIENTED USENET NEWSGROUPS

Usenet newsgroups are analogous to a community bulletin board, only they are available worldwide to anyone who has access to the Internet. There are more than 4,000 usenet news groups available on the Internet, and each covers a different topic.

Although some specific groups are moderated, usenet as a whole is not organized or administered by any one individual or organization. Adding and removing discussion forums is governed by consensus among system administrators.

Below is a list of just a few of the usenet newsgroups dedicated to:

talk.abortion—discussion and debate on the issue of abortion.

talk.politics.guns—debate pro and con on gun-control issues.

alt.activism—a discussion forum for political activists.

alt.censorship—discussion on the topic of censorship.

alt.feminism—discussion on feminist issues.

alt.politics.clinton—general discussion and debate about the President and his policies.

alt.politics.perot—general discussion about the former presidential candidate and his policies.

alt.politics.democrat—discussion and debate about Democratic party figures and policies.

altl.politics.usa.republican—discussion and debate about Republican party figures and policies.

alt.rush-limbaugh—a forum for fans and foes of the talk show host.

Senator SPECTER. Thank you very much, Mr. Berman.

We now turn to Prof. Frank Tuerkheimer, University of Wisconsin Law School.

Welcome, Professor, the floor is yours.

STATEMENT OF FRANK TUERKHEIMER, PROFESSOR, UNIVERSITY OF WISCONSIN LAW SCHOOL, MADISON, WI

Mr. TUERKHEIMER. Thank you, Senator.

Senator Specter, Senator Kohl, Senator Feinstein, I am on the faculty of the University of Wisconsin. I practice law in Madison. I am also on the advisory board to the Electronic Privacy Information Center, here in Washington.

I share the concern that there is material on the Internet that I would rather not see. I think there are things in newspapers I would rather not see. There are books I would rather not see printed.

However, I believe in a society such as ours, the answer to ideas that we don't want to see that are disseminated are ideas that we do want to see.

With respect to the Internet, I believe that it is important to realize this is simply a method of communication. It is new method. It has facilities that older methods may not have, but it is still, in the last analysis, a method of communication.

The kind of information that Senator Specter alluded to, that others have alluded to, here—terrorist manuals, how-to-do this, how-to-do that—that kind of information exists independently of the Internet. It is available. It is out there.

In the short period of time that I had to prepare my testimony, I was able to get about 12 manuals out of the engineering and agricultural libraries of the University of Wisconsin that had every bit the same kind of information in them that has been available on the Internet.

In addition, I appended onto my statement eight pages describing the use of explosives, how to make bombs, and so forth, that comes out of the Encyclopedia Britannica.

We are not dealing with information that is hard to get to. In fact, I want to bring the committee's attention specifically to a "Blaster's Handbook," that refers to ANFO, ammonium nitrate/fuel oil, the mixture that was used in the Oklahoma City catastrophe. It refers to it. It tells you exactly what the mixture is supposed to be. What percentage of this, what percentage of that. It is published by the U.S. Department of Agriculture Forestry Service.

This is information which is necessary, apparently, in the clear cutting of forest and the demolition of tree stumps and so forth.

As I think you know, explosives are used in a lawful setting far, far more frequently than they are in an unlawful setting. I mean, explosives are used in connection with road construction, with the demolition of buildings. Apparently, they are used by the Department of Agriculture, in the maintenance of forests, and so forth. We are dealing with activities that are essentially lawful.

If information relating to that is available out there in the public, I don't believe that one can say you shouldn't use the Internet for it.

Truck rentals are lawful business. I don't think you are going to hold hearings on restricting the rentals of trucks because trucks have now been used in two bombings, in the New York City, in the World Trade Center bombing, and now in Oklahoma City.

In the last analysis, I think that what this committee should focus on and what we, I think, as persons concerned with what is happening have to focus on, is (A) is there existing legislation there which can deal with this problem?

I believe Mr. Litt has referred to section 231. I am familiar with that. I am also familiar, for example, with section 1952 of the Criminal Code, which makes it a crime to use an interstate facility to carry out a designated, unlawful purpose.

So that, if someone used the Internet for purposes of facilitating the destruction of a place across the State line, for example, and used the Internet to transmit information on bombs, that, I believe, would be a violation of section 1952.

You have to, I believe, look at this statute. It is the sort of a statute that you can expand upon because it makes it a crime to use interstate facilities for designated purposes, violation of State law, for example.

If there are additional State laws that have to be tacked on to 1952, to expand it so that it covers the kind of activities we are concerned about here, I would think that that would be the way to go. However, as you can see, we are talking about regulating not the dissemination of information but information plus.

The dissemination of information for an illegal purpose and the person who uses the Internet for an illegal purpose, I believe, should be prosecuted if it can be shown that that person knows—not that the Internet is being used—but that the use of the Internet is for an illegal purpose. That would be no different than someone who makes a telephone call for that reason, someone who uses the mails in furtherance of a scheme to defraud.

It is the kind of thing that we have been dealing with for decades, for decades, and I believe with some measure of success.

Lastly, I would like to point out that we have had some success. I believe the trial which is going on right now in the southern district of New York is a tremendous example of how law enforcement can work successfully because a terrible, terrible plot—if the allegations of the indictment are to be accepted as true, an attempt to bomb the Holland and the Lincoln tunnels and various buildings in New York City—it was nipped in the bud before it happened.

Obviously, we are doing something right, and I think the challenge of these very, very difficult times is to try to react in a way where our track record remains just that. That we do the right thing and that we don't overreact and do the wrong thing.

I will be very happy to answer your questions.

[The prepared statement of Mr. Tuerkheimer follows:]

PREPARED STATEMENT OF FRANK TUERKHEIMER

I would like to thank the Committee and the Chair for the opportunity to appear before the Committee on the troublesome issue of the First Amendment and in the Internet.

The issue is troublesome because we are forced to balance a desire to avoid terrible and personal harm against abstract and nebulous concepts. This is never an easy task and certainly not made easier by arising in the immediate wake of the worst domestic terrorism incident in the history of the United States. I believe, however, that our obligation to remain true to the basic values that characterize our system of government and make it unique among the world's democracies should not be weakened by the horrors of the moment. Any effort now undertaken to deal with domestic terrorism, whether directed at the means by which information useful to terrorists is spread or expanded wiretap authority when there is no showing that existing procedures have been found inadequate, is no doubt well-intentioned. Laudatory intentions, however, are not enough to justify restrictive legislation. Mr. Justice Brandeis, in his famous dissent in *Olmstead* v. *United States,* 277 U.S. 438 (1928) warned that "experience should teach us to be most on guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty to evil-minded rulers. The greatest threats to liberty lurk in insidious encroachment by mean of zeal, well-meaning but without understanding."

The members of the committee have no doubt given much thought to these questions. I am not sure I can add much to their own deliberative processes. What I bring to the Committee is over 30 years as a lawyer, over 20 as an academic, over 10 years as a federal prosecutor, and the commitment of a professional lifetime to the values and strengths of our form of government. It is perhaps for that reason, that even while working on the Progressive case as United States Attorney for the

Western District of Wisconsin, I was probably the least enthusiastic about the case among the team of federal attorneys working on it. As you know, the *Progressive* case was the effort by the government to enjoin publication of a magazine article describing how an H-bomb was constructed. Even my limited enthusiasm waned considerably once the case took the turn of attempting to enjoin the publication of information gathered from the public domain. While the battle in that regard was won, insofar as the courts upheld the injunction, the war was lost once another journal published the same information, mooting the case, as result, I believe, that was inevitable.

The Internet is a method of communicating information, quickly, to many people and for great distances. Such communication may be in the form of a message from one person to others, distribution of information available on a public posting, or a combination of the two. What distinguishes an Internet communication from the mail, the telephone, or the voice for that matter, is the speed and breadth with which information is disseminated. In the end, however, it is just another method of communicating, and when the issue of regulating it arises, this cannot be overlooked.

Members of the Committee staff have made me aware of some of the information which has been communicated on the Internet, information which might be of great use to terrorists and others whose mission in life is the unlawful destruction of property and the taking of lives. Such information is also available to minors capable of Internet use. While no sensible person can derive satisfaction from these bare facts, I do not believe that the answer is injunctive relief against the dissemination of such information, for several reasons.

First, information is neutral in terms of what is to be done with it. Information on explosives, sent via the Internet, could be used by a company seeking a demolition contract in preparing specifications for a job offer. If time is of the essence the Internet is a more convenient form of communication than the fax since an e-mail can be down-loaded and placed directly into the specifications. On the other hand, such information can be sent for purposes of implementing a terrorist scheme resulting not in the lawful demolition of a deserted building as the first step in the construction of a new one, but in the unlawful destruction of an occupied building resulting in the large loss of lives. This suggests that any legislative effort focusing on the Internet should focus on the intent of those making the communication.

Second, the Internet is one of several methods of communication available to someone wishing to convey information. The telephone, the fax, the postal system, an overnight express service, a short-wave radio, travel and personal contact are all alternative methods of communicating. If we are concerned with a particular item being communicated, in addition to the purpose of the communication, we ought to focus on what it is that is being communicated, rather than the form of communication.

Third, the information on explosives that is transmitted via the Internet exists prior to electronic transmission; it has a life separate from the method used to communicate it. That life may be it any number of forms including a training manual for construction workers, a text-book for civil or mining engineers, and a general explanatory text on explosives in an encyclopedia. Attached to this statement is a copy of pages 275–282 of Volume 21 of the 1986 Encyclopedia Britannica. It reveals great detail on explosive manufacture, similar in many respects to the information disseminated electronically of concern to the Committee and others, including, on page 279, a description of the Ammonium Nitrate/Fuel Oil mixture used in the Oklahoma City bombing. Also attached is a list of books containing similar information to the kind transmitted electronically. The books on this list were obtained from the Engineering and Agriculture libraries at the University of Wisconsin in the one day between the invitation to appear before this Committee and the preparation of this statement and are generally available. Among these books is a "Blasters Handbook" published by the Department of Agriculture Forestry Service which in turn includes a description of the Ammonium Nitrate/Fuel Oil explosive used in Oklahoma City along with the recommended mixture of the two chemicals. The widespread availability of information whose electronic transmission is to be enjoined argues conclusively, in my opinion, against such extraordinary exercise of government power.[1]

Finally, children do not have access willy-nilly to information on the Internet, certainly not more so than to comparable information available elsewhere in libraries and encyclopedias. A child either savvy in the use of a public library or just smart enough to ask a librarian for help can easily find the same kind of information available on the Internet; indeed, such information is available to the public as a whole without the need for any capital investment or technological skill. Children

[1] The attachments submitted by Mr. Tuerkheimer were retained in the committee files.

who can obtain access to terrorist manuals on the Internet presumably live in homes where computers and modems are in use; if parents are concerned their children will obtain information they can use for the wrong purposes, they can take steps in insure that their children do not do so. Despite the distressing number of accidents involving children and firearms, in all the discussion on regulation of firearms, no one has yet proposed that people with children in the house be prohibited from owning guns.

The thrust of these observations is that if Congress proposes to deal with the use of the Internet for illegal purposes, it should do so in the same manner it has dealt with the use of other federal instrumentalities and facilities of interstate commerce used for illegal purposes. For example, it is a crime

(1) To use the mails in furtherance of a scheme to defraud (18 U.S.C. sec. 1341),

(2) To use wire facilities in furtherance of a scheme to defraud (18 U.S.C. sec. 1343),

(3) To transport an explosive in interstate commerce with intent to unlawfully damage a building (18 U.S.C. sec. 844)

(4) To travel in interstate commerce *or use any facility in interstate commerce* with intent to facilitate designated illegal activity (18 U.S.C. sec. 1952)

(5) To transmit in interstate commerce any threat to injure another (18 U.S.C. sec. 875)

These are just five examples of a legion available in Title 18 of the United States Code reflecting the Congressional use of its jurisdiction over interstate facilities to deal with criminality involving the use of such facilities.

With these existing statutes as a guide, upon a showing of need and the absence of applicable legislation, Congress could consider a law making illegal the dissemination of information via an electronic media by a person who has knowledge that the dissemination of such information is in furtherance of designated criminal activity. Such a law would be far more effective than an effort to obtain a prior restraint on the dissemination of information. This is so for several reasons.

First, it would permit the arrest of the person seeking to disseminate such information, thereby assuring not just that the Internet will not be used for the prohibited purpose but *any* method of communication since the person himself or herself will not be able to utilize alternate methods of communication from jail.

Second, criminalization and arrest are superior to a prior restraint in that they are more effective. It is difficult to envisage a type of person who is prepared to use the Internet to further illegal activity compliantly stopping once served with a court order directing that there be no communication. When engaged in conduct involving serious criminal penalties, the threat of a contempt of court citation is not exactly bone-chilling.

Third, by focusing on the purpose of the person using the Internet, the risk of needless government interference with legitimate activities is significantly minimized. Such government interference is not to be undertaken lightly. Mr. Justice Hughes in *Near* v. *Minnesota,* 283 U.S. 697, 716 (1931) made it explicit: "any system of prior restraint comes to the Court bearing a heavy presumption against its constitutional validity." Even governmental assertions of damage to national security during the Vietnam War did not overcome that presumption. *New York Times* v. *United States,* 403 U.S. 713 (1971) ("Pentagon Papers case"). It would appear far wiser for Congress to focus on illegally motivated conduct rather than the technology used to communicate information.

There have been very few prior restraints in our history precisely because of the directives of the First Amendment. While technological changes create challenges to a society operating under the First Amendment, they also give power to the government vastly beyond anything the framers of the Amendment could have imagined when it was drafted. This underscores the importance of the First Amendment and the ongoing need to pay heed to its constraints.

Senator SPECTER. Thank you all very much.

Professor Tuerkheimer, permit me to begin with you. When you point out that the Internet is just a means of communication and that these manuals are available other places, you are exactly right about that. And part of our inquiry is beyond the Internet, to the dissemination of the materials.

The seminal leading case is *Brandenburg,* where the Supreme Court handed down the doctrine of the imminence of violence, so that freedom of speech is protected.

I think it is important to look at the factual context of Brandenburg, which was an Ohio criminal syndicate act, which on its face purported to punish mere advocacy. The kind of language used in *Brandenburg*—scattered phrases derogatory of African-Americans and of Jews, and a film of six hooded figures—relatively little by way of anything approaching danger to the public.

Justice Jackson uttered the famous comment that the Constitution is not a suicide pact. I think history has served us well in broad interpretations of the first amendment. There is no question about that.

Take a look at what is going on, now, with the imminence of violence and the problems of terrorism, domestically, and the availability of the information and its access to very young people, the case that you handed back in 1978–79, in the Federal court in Wisconsin, did involve a prior restraint, the only one on record, as least as of that time, as noted in the judge's opinion.

That court took a look at other rights. The right to life, liberty, and the pursuit of happiness, as the court balanced off other rights under the Constitution.

You have suggested in your written testimony that there could be statutes which would preclude the dissemination of information by a person who has knowledge that the dissemination of such information is in furtherance of designated criminal activity.

My question to you is, what did you learn from your own participation in the case involving the hydrogen bomb, which was simply the description of how to use it? The Atomic Energy Act was implicated, but there was no imminence of detonation of a hydrogen bomb.

What lesson does that have, if any, in a broader context for other bomb manuals?

Mr. TUERKHEIMER. Senator, I believe that the lesson of the hydrogen bomb case is that efforts to curtail the dissemination of ideas and thoughts by means of an injunction are doomed to fail.

While the hydrogen bomb case was successful in terms of the law, an injunction was obtained, it was affirmed by the seventh circuit, the information got out.

The same information that was contained in the article whose publication was enjoined was published elsewhere. The end of the case was the dismissal of the complaint on the grounds of mootness.

I don't believe you can effectively deal with the dissemination of information by enjoining its dissemination. It is just not going to work in an open society.

As far as I am concerned the lesson of the H-bomb case is, that is the wrong way to go.

Senator SPECTER. Would the facts of your H-bomb case have supported the criminal prosecution for the person who was disseminating the information?

Mr. TUERKHEIMER. Not even close, in my opinion. It is not even close, because the very fact that the information is out there makes it very difficult to show that there is any real injury to natural security.

If a defendant in a case of that sort would have been able to show that everything that was in this article, whose publication is

supposedly injurious of national security, it is all out there, including in Government libraries.

There was a library in New Mexico that contained much, much of the same information that was in this article that the Government sought to enjoin. The criminal case goes down the tubes.

Senator SPECTER. Mr. Litt, are you able to shed any light on the extent to which bombs are actually made by reference to these manuals?

There was an NBC television show which dealt in some detail with what was going on in North Jersey on the subject. Would you have any factual matters to offer the committee on that?

Mr. LITT. I don't think that it is really possible to get a grip on what people are using the Internet to make bombs, what people are using the published manuals to make bombs.

Bombs are being made. There are numerous cases that have happened for years and years of people just using the published manuals. There is no doubt that there are people who are downloading information from the Internet and using this to experiment with bombs, but I don't think we have any solid information as to a particular number of cases in that area.

Senator SPECTER. Well, I think there are a number of cases where the investigation after the explosion has led to the discovery of the manuals which were used in the construction of the bombs themselves.

Mr. LITT. As I said, there is no doubt that this does happen, but I don't think we have an ability to assess, at this point, how many people get information off the Internet, how many people get it from other sources.

Senator SPECTER. Well, aside from the Internet, it would be helpful to the committee and the subcommittee, if the Department of Justice would make an effort to give us some sort of a factual basis as to any connection between these manuals and the actual construction of a bomb which was then used in some sort of criminal activity.

Mr. LITT. I will see if we can get you that information.

Senator SPECTER. OK, thank you very much. My time has expired. Senator Kohl.

Senator KOHL. Thank you very much, Senator Specter.

Mr. Burrington, if you recall, in my statement, I suggested that the online services that help connect people to the Internet take several steps to protect children.

I mentioned things like notification of parents when their child opens up an account. Parents should be able to keep their kids off parts of the Internet and the online industry should look to the video game industry to prevent access to minors.

Are these recommendations feasible, are they advisable? What is your reaction?

Mr. BURRINGTON. Senator, I think, first of all, a number of these things, we are already doing actually as an industry. Let me point your attention to a couple things we attach as an appendix to our testimony. The "Child Safety on the Information Highway," a brochure which we publish by the thousands and it is available electronically to our members. It was published by the ISA and the National Center for Missing and Exploited Children.

Part of the problem we have here, which you correctly point out, Senator Kohl, is that younger people are certainly more computer literate, I think, than perhaps their parents are, who can't set the time on their VCR. And so, we are very aware of that and we are trying to work in a way that—for example, at America Online, when you are an account holder, to be a primary account holder, you must be 18 years of age or older, so that you can't even sign on to America Online and get an account on our service unless you are over 18, to be the primary account holder where the bill is sent. That is one thing.

Second, we have—and a lot of the services have—what are called parental control mechanisms. It is technology, actually, that we are using to help deal with this.

At America Online, if you are a family of five, you can have up to five screen names on your service. You can actually go in and decide for your 13-year-old son that he is going to be excluded from certain areas on our service and it allows parents, actually, to block their children from certain areas.

I think, over time here, and the reason we have been encouraged by the attention to this issue, both by Senator Exon and his legislation and also Senator Leahy, the bill that you cosponsored, a study of these issues is very critical because they are very complex.

What we would like to see, here, is a combination of industry working with government, working with consumer groups, working with the Rabbi's organization, to use education, to use technology tools, to help get at some of these concerns, which is protecting children.

I would just urge you, Senator, and the subcommittee, that we be very careful not to cast too wide of a net over the net in an attempt to get at some things we don't like.

Senator KOHL. Yes, Mr. Berman.

Mr. BERMAN. Thank you. At this point, we are working on a study along with America Online and long-distance companies, other information providers, content providers, to try and bring together the technology potential in this area.

The Center for Democracy and Technology is coordinating that study. It is a preliminary one which we hope to elaborate more if the Senator Leahy study can get going.

And maybe, we are prepared to have a demonstration for the committee in the near future of some of those technologies. We have been contacted by many companies—I don't want to use proprietary names, but there are lots of things in the works which will give navigational tools for parents and for online services that can keep children out of offensive material—and that is just not sexually explicit, but violent, commercial, noncommercial—and I think that we are looking to the potential of this technology to give users control over what they want to watch and what their children want to interact with as a way to argue that the Internet is a new kind of speech milieu and that it is better to approach it from that user control than to impose content restrictions, as we do with mass media.

So, there is a win-win here for free speech and for parental control if we can forward this study and bring industry forward to show what can be done and what is in the works.

Mr. BURRINGTON. Senator, if I may, your comment about the industry should get the message and act now or Congress will, I think, is well taken.

That is why we are working with the Center for Democracy and Technology, through the ISA, I think, to deal with these issues. They are complicated because it is one thing when we talk about America Online, because we are a closed service, and we can control somewhat what happens on our service.

You get a contract when you sign up with our service. We have terms of service. If you violate those terms, you can be kicked off of our service.

But once you get out in the big sea of the Internet, that is a whole other world and it literally is the world. That is going to be really tough when we talk about regulating content on the Internet because what we do here in the United States won't necessarily work elsewhere.

Mr. BERMAN. Let me make one point of clarification, which I think you really do have to understand.

The service providers, like America Online and CompuServe, they are closed systems and they have subscribers and they can monitor what is going on, on their networks. But increasingly, the Internet—they really are not the Internet. The Internet is this network of networks which has no control. The Government started the network and now it is becoming commercially viable, and there are many, many providers, and it means that it is very easy to go directly to the Internet, reach thousands and thousands of sites around the world.

For example, the terrorist manual that we downloaded was in Britain. Another one, "How to Make a Bomb," was in Sweden. So, it is a world network, and the idea that we are going to build a wall to keep out bits, in computer terminology, I think, is a losing effort. That we really do have to look at our ability at the consumer end to control and filter information that we want our children to see or which we may want to see or not see.

Senator KOHL. Any other comments? Mr. Hier.

Rabbi HIER. Yes. I would just want to point out, Senator, that with reference to the comment that the information is out there, anyway, that is true, but not quite on the same level.

It is quite different when you own a network. This is the opportunity of a hater, a bigot, and it is his opportunity to speak to the world. It is not the same as if we have manuals, like the Militia of Montana Manual, available in a bookstore. I think the comparison is not an accurate comparison.

Second, I think that we do have a responsibility both ways. Freedom of speech should be protected, but on the other hand, society should not allow ourselves to be excused from our own responsibilities.

I do not believe a neo-Nazi group can pay for an ad on CNN and that CNN will accept the ad. They can come up with the money and say we want 1 minute of your time and we are going to tell America what we believe in, and I believe that CNN will turn the ad down.

So, there are responsibilities for providers. We have worked with Prodigy very closely and, I may say, that we have successfully

worked with Prodigy to point out to them the areas of danger when you simply allow haters to have a free pulpit.

I will just close with this. One of the true remarks, unfortunately, that Adolf Hitler once made, when commenting on how his early movement was very successful, he credited it entirely to his understanding of technology and how to make use of it. He was the first to use the new Gestetner machine and the first to place his organization's ad in the mainstream newspaper.

Haters know how to use technology and the rest of society can't just sit back and say we will give them the freedom to operate as they see fit and our response will simply be that we watch from the bleachers.

We have responsibilities, too. We should exercise them.

Senator KOHL. All right. My time is up, Senator Feinstein.

Senator FEINSTEIN. I thank you very much, Senator.

I am not an attorney, but I must just tell you, the only one I agree with is Rabbi Hier. I have real problems with what has been said this morning.

If I follow the thinking through to its logical conclusion, you can have a prime time show on network television, like a cooking show, on how to make a bomb, with specific directions of how to steal the chemicals, where to get them, how to pick the lock and what to pick the lock with. How to put the bomb together. How to be careful so that you are not wounded by that bomb. All on network television.

What you gentlemen, in my opinion, are espousing is a pushing of the envelope to extremes, and I must just tell you that.

I am looking at some of the things on a baby-food bomb, how to destroy a car, with a store to go to to get the specific bullets, where to find them by the hunting section, with a diagram of how to cut the bullet, how to put an antipersonnel device on it, using sharpened jacks because the good thing about those is that any side the bomb would land on is the right side up. If the explosion doesn't get them, the glass will. If the glass doesn't get them, the nails will.

I think you are engaging in the promotion of an ultra-hazardous pursuit. You are a purveyor of this stuff.

Then, you go on to how to break into a chemical lab in a college, how to pick the lock of the door, how to commit crime after crime after crime, and you are using your first amendment right to justify its purveying.

Now, I have listened very carefully and you've got my dander up, so you got to listen to me, a little bit.

I am a mother and a grandmother. I don't want my kids to have access to this stuff, and I don't consider it part of their first amendment right.

When my daughter came to me and took a cookie when I told her not to do it, and she said, "Other kids do it, it is OK, Mommy"

I said, "It is not OK for you."

I have a hard time with people using their first amendment rights to teach others how to go out and kill and to purvey that all over the world.

I must tell you, that is not what this Nation is all about.

Mr. BERMAN. May I respond?

Senator FEINSTEIN. Absolutely, you can respond, but I am just so appalled.

Mr. BERMAN. Protecting that speech is what this Nation is about. I am sorry. Are you proposing that we outlaw speech of that kind? In other words, for bookstores?

I mean, it is not just network television. We are talking about bookstores. We are talking about libraries. We are talking about a worldwide information environment.

We have gone through periods where we tried to fight speech by criminalizing it, and that has not been exactly the best times of this country.

The best way to deal with speech is with more speech. The best way to isolate people who build bombs or who think that terrorist manuals are the way to go is to convince them that there is an open society, that there is an open debate, that there is a free speech, that there is an Internet where people can use it, that we do believe in a wide-open, free-flow of information, and that gives the lie to terrorist plots or the idea that you have to be paranoid about the Government because it is clamping down on your right to dissent or to change Government by lawful means.

Senator FEINSTEIN. If I may, Mr. Berman. I believe there is a difference in free speech and teaching someone how to kill others. That is the only purpose for a bomb, to kill.

It is not to look at. It is to kill.

And we are teaching someone how to kill, and that is what these diagrams do. That is what the rhetoric behind them does. Not just to learn, but to kill.

The language is incendiary; it is not academic. We are protecting this with the mantle of free speech.

I think, as a nation, we have to come to grips with this. There is no nation on Earth that is freer than ours. No nation at all.

I have just watched, over the decades, as the envelope gets pushed and pushed and pushed and this society is subject to more violence from within it.

It is all under the guise—and I think that the doctrine of prior restraint is one that we really need to look to, and I think we really need to, frankly, examine our conscience as to whether this is how we want to raise our kids, learning how to build bombs, blow up other people.

Mr. TUERKHEIMER. May I?

Senator FEINSTEIN. Sure, have at it.

Mr. TUERKHEIMER. Well, Senator, I don't think there is anyone in this room who is happy about the dissemination of the kind of information in the form that you describe. I don't believe it.

However, I think that before we think about giving the Government the power to curtail the dissemination of this kind of information—and that is a power. It is a power that is significant and could significantly change our society.

I would think that the first thing that you would want to do is, rather than have a generalized distaste or dislike for that kind of information, you would want to be pretty sure that it has actually caused injury.

I don't believe that the record is out there to come anywhere close to that. I don't believe that there is any showing, for example,

that the persons who were involved in the World Trade Center bombing were inspired by information that they read in books or that they saw on television or received over the Internet, or that the Internet, or any particular means of modern communication——

Senator FEINSTEIN. So you are saying, let me see if I understand you, that you need to be shown that there is a direct cause and effect, with specificity, between something that is on the Internet and written, that the exact components——

Mr. TUERKHEIMER. Well, it doesn't just have to be the Internet. It can be anywhere.

But I think, yes, you would want to see that there is a harm here, beyond just what we might——

Senator FEINSTEIN. And you don't believe that there is? You don't see the connections?

Mr. TUERKHEIMER. I don't think there is anything out there indicating that the freeness of our society and the ready access to the kind of information you are talking about has resulted in injury.

Now, you say that bombs are designed to kill people. I would think that for every bomb that is detonated that kills people, there are probably a thousand bombs that are detonated for a lawful purpose.

I mean, the Department of Agriculture is not in the business of abetting illegal activity. There are significantly lawful purposes for which this information is used and if those people engage in those lawful activities want to use modern technology, what is the problem?

Senator FEINSTEIN. So what you are saying is that the first amendment—and my time is up. I will just finish this.

That the first amendment, basically, enables you to teach others how to build bombs, put it up on a billboard, the formula, put it on network television, put it on the network, teach it in schools. That this is all within our first amendment right, how to kill.

Mr. TUERKHEIMER. I don't know that teaching it in schools would be within the first amendment. There are obviously different constraints that operate there.

No one has the right to go into a social studies classroom and instruct children on how to make bombs.

But I think as a general matter, yes, I mean the fact of the matter is, the first amendment—if it means anything, it means that one has the power to disseminate obnoxious ideas. That is really the test of it, and that is what makes our country different from virtually every other country in the world.

That we use the marketplace as a vehicle for controlling people's thoughts, we don't use government.

Mr. BURRINGTON. Senator, may I have——

Senator FEINSTEIN. My time is up, Mr. Chairman.

Senator SPECTER. Go ahead, Mr. Burrington.

Mr. BURRINGTON. Thank you, Mr. Chairman.

I am very sensitive to, and I appreciate, your concerns. As a parent, they are legitimate concerns. We hear those concerns a lot.

Let me try to draw a different analogy. There is the book, "Final Exit," which was a nationwide bestseller, which is sort of a sad

commentary, perhaps, on our society. But it was, nonetheless, a nationwide best seller on how to commit suicide.

It was carried in every bookstore in this country. And yet, committing suicide is illegal in many States. We were teaching people how to kill themselves.

It is not good. It is not nice, but you had a choice whether you wanted to buy the book or not.

You raise some critical issues, here, and this is why, I think, we are supportive of Senator Leahy's approach and others, to take a look at these issues because there is no quick and easy fix here, by any means.

At America Online or with some other members who are private, commercial services, yeah, we could say: We don't want books on bomb making or manuals on bomb making, so we are not going to allow them on our network. But you are off into the Internet, which is a global network, you lose that control.

I mean, we can try to stop it here, but what are we going to do about the manuals that are coming from Sweden and Britain?

You know, there are no geographic boundaries to this network. We don't have a border, so to speak, so those are some very tough issues.

Finally, I want to emphasize here that we are focusing on bombmaking manuals, but the vast majority—there is a sea of information out there—that improves people's lives, that actually helps people live fuller lives and better lives, and I want to make sure that that point is not lost here. That as we are, again, trying to cast a net over the net, that we don't go after a small fraction of information and overlook the fact that this technology and this new communications medium is improving the quality of people's lives. It is bringing our country closer together, and it is bringing the world closer together.

It is just a counter balance, Senator, to your other, legitimate concerns.

Senator FEINSTEIN. Thank you. Thank you, Mr. Chairman.

Senator SPECTER. Thank you, Senator Feinstein.

Professor Tuerkheimer, pursuing the line of questioning which Senator Feinstein was on, there is no doubt about the first amendment protection of ideas. There has been a considerable amount of writing on the protection given to ideas distinguished from a manual-type operation. In a sense, having a manual on how to make bombs is not the articulation of ideas.

Would that formulate any distinction in your mind for a little different analysis as to the application of the first amendment?

Mr. TUERKHEIMER. I don't see how you can do it. I don't see how you can take the combination of thoughts as to how things are done, which are then put into writing or some other format that is published, and say Government can regulate it.

If you don't have the immediacy of injury that Brandenburg talks about or the earlier "clear and present danger" test.

These are thoughts on how things are done, and I believe that absent any kind of immediate injury, I think under the first amendment, you have to let it go.

Senator SPECTER. Well, how about your suggestion about making criminal activity by a person who has knowledge that the dissemi-

nation of such information is in furtherance of a designated criminal activity? What do you have in mind, there?

That, as your written statement suggests, is a little different from the kind of imminence which *Brandenburg* talks about.

Mr. TUERKHEIMER. Oh, but I think there is specific injury that is contemplated.

If I am making a speech to a bunch of people who say, "Hey, we want to blow up the Federal courthouse in San Antonio," or "We want to set off a bomb on a Presidential caravan or route when they come through Des Moines," or whatever, "Can you help us out"?

And I say, "Sure, here is what you have to do. Here is how you put the bomb together." That kind of thing, seems to me that that kind of thing can be regulated and can be proscribed and could be made criminal and punished with great severity, and ought to be.

Because the point is, when I make the communication, when I transmit thoughts as to how bombs should be made, I know that I am facilitating the commission of a crime. I am making it easier for people who are listening to me to carry out a crime that I know they want to carry out, and yes, I should be prosecuted for that.

Mr. LITT. Mr. Chairman, if I can just add a comment there?

Senator SPECTER. Go ahead.

Mr. LITT. I believe that the example that you and Professor Tuerkheimer are talking about is already illegal under existing laws relating to conspiracy and aiding and abetting.

If somebody comes up to me and says, "I want to blow up the Federal building, can you teach me how to make a bomb?" That person is easily prosecutable within the scope of existing law, regardless of the fact that the means in which the offense was carried out constituted speech.

In fact, in the pending trial in New York involving the World Trade Center, a motion to dismiss the indictment was made by Sheik Rahman on the grounds that his conduct was protected speech. The court had no trouble rejecting it on the grounds that even if you speak, if your acts thereby constitute a crime, you can be punished for it.

Senator SPECTER. Mr. Litt, to what extent, if at all, do you think that easy access on how to make bombs or explosive devices constitutes a threat to public safety?

Mr. LITT. I don't think there can be any doubt that it does constitute some degree of a threat to public safety.

I also think that those people who are dedicated to committing a criminal act are going to find this information out in one fashion or another. That the terrorist, who was intent upon blowing up a building, and wants to find a way to do that, will find that information somehow.

Senator SPECTER. To what extent is there a problem other than from the dedicated terrorist? The 13-year-old who finds ready instruction on how to make a molotov cocktail?

Mr. LITT. I think there is absolutely a concern with respect to the availability of this information to children, and I think Mr. Burrington mentioned before that the Department and the Members of Congress and the online industry are looking at ways to see

whether it is possible to limit the access of children to information on the Internet that they shouldn't have access to.

Rabbi HIER. Senator, may I?

Senator SPECTER. Certainly, Rabbi Hier.

Rabbi HIER. I would like to read something, and I think this will go directly to your previous question, Senator.

This came on the Internet through America Online. This is a quote.

> I want to make bombs and kill evil zionist people in the government. Teach me. Give me text files! SOF materials are on the way. . . . Feed me your wisdom, Oh, great one.

Now, somebody——

Senator SPECTER. Rabbi Hier, are you now reading from a message which was put on the Internet seeking information?

Rabbi HIER. It is in the documents that we provided on page 9, where a person says, "I want to make bombs and kill evil zionist people in the government." Page 9 of the documents.

That would be an example of a person that uses the Internet, seeking information on how to make a bomb to kill people, specific people, in the Government.

My point that was made previously, Senator, while I don't believe you were here when I made this point, and that is, that there is also a responsibility on the part of providers and we simply cannot shirk the responsibility by saying we all support the first amendment and nobody wants to curtail the first amendment.

But, I don't hear too many people speaking about what the responsibility of the providers. Do we have to give them the main access to society or should they continue to be marginalized, as is the case, in network television? As in the case of all other areas when we deal with hate groups?

And by the way, I might say, with reference to a previous comment about using the Internet, that the Internet is widely dispersed beyond just the providers. Recently, somebody was using the Internet under the name of the University of Texas to send out hate material.

The University of Texas did not know this. When the university was alerted that somebody at the university, a student, was using the university Web to disperse hate material, the university just exercised its responsibility and said, "That is not what the University of Texas Web is all about," and it stopped it.

That is called exercising responsibility.

Senator SPECTER. Rabbi Hier, when you make reference to this message, "I want to make bombs and kill evil zionist people in the government. Teach me. Give me text files! SOF materials are on the way . . ."

That is by the same person——

Rabbi HIER. That's correct.

Senator SPECTER. "Feed me your wisdom, Oh great one."

Rabbi HIER. Right.

Senator SPECTER. Do you happen to know what response there was, if any, to that?

Rabbi HIER. I don't believe that we were able to—we did not receive the response. We could not track the response.

But there are many, many other examples on the documents that we provided where people are using the Internet threatening others.

In other words, I think it would be very hard-put to say why an obscene phone call is illegal when you are threatening a specific individual, and here you have people that are using the Internet in an attempt to also threaten people, and to simply say that that is excused and that we have no way of dealing with it.

Senator SPECTER. Mr. Litt, if somebody responded to this request, telling the enquirer how to make bombs to kill, would that person giving the information be chargeable with a criminal offense?

Mr. LITT. As I am sure you can understand, I am hesitant to give prosecutive opinions under these circumstances, but it would certainly seem to me that that is at least approaching, if it has not already crossed the line, into criminal activity. There are statutes that, by themselves, prohibit the use of interstate facilities, including the Internet, to make threats.

It would seem to me that the kind of activity that is described there, particularly if somebody responds with a specific instruction, might well be something that was prosecutable under existing law.

Senator SPECTER. What do you think, Mr. Berman? Would that constitute a criminal violation?

Mr. BERMAN. I think it is still speech. We don't know who the person is, whether that person is just a disturbed person or—there are many, many, many people out there saying crazy things. There are children posing as adults, adults posing as children.

Just simply going on the basis of Internet information, you would be targeting thousands and thousands of people for investigation and potential prosecution because there are many incendiary things——

Senator SPECTER. I am not talking about investigations. I am talking about the hypothetical where you find the person who provides the information to make the bomb in response to this request. And that would not constitute a criminal act, in your opinion?

Mr. BERMAN. Not the hypothetical—if you would like to read it to me, one more time.

Senator SPECTER. Well, it is not a hypothetical. This is an actual message.

Mr. BERMAN. Send me——

Senator SPECTER. The hypothetical part is when I add that there is someone who responds to this message by giving them the material.

The message is, "I want to make bombs and kill evil zionist people in the government. Teach me. Give me text files! SOF materials are on the way. . . . Feed me your wisdom, Oh great one."

Mr. BERMAN. I don't think that is a prosecutable offense. I don't think it is imminent laws action. I think it is——

Senator SPECTER. I am not talking about this request, I am talking about someone who would then provide the information on the Internet as to how to make the bomb.

Mr. BURRINGTON. Senator, I am not a criminal law expert, so maybe this is a stupid thing to try to——

Senator SPECTER. Well, just a minute, Mr. Burrington.

Mr. BURRINGTON. Yes.

Senator SPECTER. The question is pending for Mr. Berman.

Mr. BURRINGTON. Yes, OK. All right, fine.

Mr. BERMAN. I would want to know more of the facts about this case. I would want to know who is speaking. I would want to know the context in which the message—whether people are sending—I would want to know what information is sent back.

But, if—yes. If you have, you know, "kill zionist people," and you send him a hard-core, how to build a bomb, there may be a case, there.

Senator SPECTER. There may be a case, there.

Mr. BERMAN. Yes.

Senator SPECTER. If there is a case there, Mr. Burrington—we will turn to you, now—on your area of expertise, Internet.

Could the Internet stop a reply from coming back?

Mr. BURRINGTON. It is a good question, sir. Let me draw the distinction, here.

Because the Internet itself, this thing, that has taken on a life of its own, could not. All right? It is a network of network computers with a community of up to 30 million people out there and there are bound to be some real nut cases.

With respect to America Online, and in this case, this was a—it looks, from looking at this—that this was a message that was pulled off the Internet, all right, somewhere. The message could have originated wherever, I think, and then it was posted on our system.

In that case, we could remove that, that message, and we do remove messages like that.

We get a lot of complaints from, you know, we will get e-mails from people saying, "This is out there," whatever.

Senator SPECTER. To what extent are you able to watch those messages to remove them?

Mr. BURRINGTON. We cannot, under the Electronic Communications Privacy Act, in terms of private e-mail, we cannot, and we will not, because it is against the law, unless we are subpoenaed. And we are sometimes subpoenaed by Federal or State law enforcement officials.

Senator SPECTER. In the context of when this kind of a message appears——

Mr. BURRINGTON. On a public bulletin board or sort of a public posting, in this sense?

Senator SPECTER. Well, that is what it appears to be.

Mr. BURRINGTON. Right, that is correct.

Senator SPECTER. Then you do have the authority to remove that?

Mr. BURRINGTON. Yes, we do.

Senator SPECTER. So my pending question to you is, to what extent can you observe these kinds of messages to effectuate a prompt removal? That is, precluding someone from replying?

Mr. BURRINGTON. There are literally tens of thousands of these messages a day posted and we do have people, at least—I am speaking, now, solely for America Online—but we do have people who are sort of monitors that do specialize in certain of our chat

areas, for example, just to generally check to make sure that there are not any violations of our terms of service.

We list in our terms of service, a whole range of things that are not permissible. Obviously, anything that would advocate——

Senator SPECTER. I don't quite understand your answer. How many people do you have looking at how many messages to get some idea as to the practicality of taking it off the message line?

Mr. BURRINGTON. It is impractical for us, given the volume, just on our own closed service, to have people monitor and look at every single thing going through our network.

What we do do, though, is, we have people trained in certain areas, particularly like children's areas and other areas to sort of monitor what is going on, and when they are made aware of something that is deemed to be a violation of our terms of service, then that message will be removed.

We generally give that—it is a "three strikes and you are out" policy. You will get a warning twice and then you are moved from the system.

Senator SPECTER. But as you say, you really can't police this sort of thing. There are just too many messages up on the Internet.

Mr. BURRINGTON. It is practically impossible. Certainly, on the Internet, we cannot. Once we get out into that sea of information, we simply cannot.

Senator SPECTER. Professor Tuerkheimer, does that constitute a crime, to respond to this kind of a message with materials on how to make a bomb, in your judgment?

Mr. TUERKHEIMER. I cannot see the FBI and the U.S. attorney's office taking a personal response to that kind of a generalized request for information and going ahead and making a criminal case.

Senator SPECTER. I am not talking about the request, I am talking about someone who would respond.

Mr. TUERKHEIMER. Taking the response to the request.

Senator SPECTER. Response, providing the information on a bomb.

Mr. TUERKHEIMER. I don't think they would do it. I think it is too generalized, though. I think if there were——

Senator SPECTER. What do you mean, too generalized?

Mr. TUERKHEIMER. If there were a name. "I want to kill so-and-so. Help me."

And then, the person provides information. I think that would easily be prosecutable, and would be prosecuted.

Mr. BERMAN. Let me make one more——

Senator SPECTER. Just a second, Mr. Berman.

You think the absence of a specified target eliminates the possibility of a prima facie case?

Mr. TUERKHEIMER. I think that is correct. I think you are close to the line and it is obviously uncomfortable. It is a difficult question, but I think the answer to it is that as long as the request for information is as generalized as we are dealing with, here, I don't think the response to it involves assistance in the commission of a crime that would be prosecuted.

Senator SPECTER. Mr. Litt, do you think you have to have a designated target to have a prima facie case?

Mr. LITT. Well, we are dealing with a question of line drawing, here, obviously, and this is why I said that——

Senator SPECTER. Well, it is really more than line drawing. We are really trying to get a feel for what we have and a feel for what the problems are and a feel for what ought to be done about them, and perhaps the answer is with Internet, itself, on some technical line.

You have these "mayhem manuals" out there as a generalization so the consensus is, notwithstanding Senator Feinstein's concerns, that that is protected speech. It is not really an idea. But, that it is protected speech.

But then, you add to that someone who comes on the Internet and says, "I want to make bombs and kill evil zionist people in the government."

Now, if the information on how to make a bomb is out there in the abstract and it is not in response to this request, well then, it is in the idea category.

But if someone responds to this and says, "Here is the way to do it," do you have to have a specific evil zionist in mind?

Mr. LITT. I wasn't trying to duck your question before by saying we were dealing with line drawing. I don't think that there is any per se requirement that to be prosecutable there has to be a specific named individual. But I think that, again, the investigative agency and the U.S. attorney would probably want to know more about the surrounding circumstances.

In answer to the direct question, I don't believe that there is a specific requirement that an individual be named as the target of a threat.

Senator SPECTER. Mr. Berman, I will come to you in just a minute.

Mr. Burrington, is it possible to have more observation of what is online to take this kind of an inquiry off, to try to at least eliminate somebody who is asking for the information?

How tough would that be for you to do?

Mr. BURRINGTON. In the context of a closed, private, online network, like America Online, we have an easier shot at doing that. It is still going to be very difficult.

As we grow, we have a community of 2.5 million people right now, and it is growing, and so, it is very difficult.

The problem is, Senator, we also offer a gateway to the Internet. Once you do that—I use the analogy, it is like being at a resort and we are the private swimming pool, and then you cross the street into the ocean, and that is the Internet.

We can have lifeguards, to some extent, and we can have lane barriers and other things in our closed pool of information, but when you cross the street into that vast sea of information which is the Internet, we have no control over it.

And so, in this case, I am not even sure—and perhaps Jerry can identify where this came from—but, I mean, who knows? That is part of the problem.

If you are going along a line, Senator, of asking private, commercial, online services to have to have little technicians, you know, sitting in front of screens, monitoring every single message being posted, it is just simply——

Senator SPECTER. You just can't do it. I can understand that.

Mr. BURRINGTON. Yes.

Senator SPECTER. Mr. Berman, you had a comment?

Mr. BERMAN. Just a couple of comments. I was not taking this lightly, but only in the context of how the Internet works. Messages like this, people do not—if they are serious about things, they don't publish on bulletin boards information like this and they don't get replies on a public bulletin board, saying, "Here is the bomb information that you want."

These transactions are going to happen in private e-mail, which are not going to be visible to AOL or anyone else. It is going to happen that way.

People are going to use it just like a telephone call. They are going to send private messages between each other and the response is not going to be visible.

The other way that the Internet is working is that this kind of generalized, "send me information," is not the way someone who wanted a bomb would get it, now. There are 37,000 Web sites, now, which are—people are just putting up their own storefronts and it is going to grow and grow and grow, and what will happen is that someone who wants to publish manuals will have, you know, a Web site called, "Terrorist Manuals," or "Bomb Manuals," and they won't be engaged in sending information back. It will just be this person will come to that site and take it down.

There won't be a transaction that prosecutors can go after.

You are not going to get a case like this, sitting out there on the Internet. That is not the way it works.

That is why I didn't take it seriously. It is not the way it works.

Rabbi HIER. Senator.

Senator SPECTER. Well, you may not get a case or you may, but for purposes of our hearing, what we are trying to determine is what are the outer bounds? Where can law enforcement act? Where do you cross the line? Rabbi Hier.

Rabbi HIER. Senator, one of the reasons that I brought that forth is that, in my remarks, I brought up the aspect of giving the authorities, the FBI, the right, when somebody sends a message of that nature over the Internet, I believe it concerns—it should concern—the Justice Department and the FBI. Because we can't simply say, "Well, the guy is probably a crackpot, and let's just dismiss it out of hand."

So, first amendment rights absolutely have to be protected because that is what our country is all about. But having said that, I think that if somebody puts this out on the Internet, there should be authority for the FBI to immediately try to find out is this serious? And to watch and to see and to monitor whether or not such a response would come forth.

I do not believe that that violates anybody's first amendment rights because the authority of the FBI is to prevent acts of terrorism of this nature.

What if the person is simply telling the truth? And what if somebody supplies him with the information, but the investigative authorities have no authority to look into the matter?

Mr. LITT. Mr. Chairman, can I just say something in that regard?

Senator SPECTER. Sure.

Mr. LITT. I believe that the FBI already has the authority to investigate a communication like that and that it could be presented to the local FBI office and they would have the authority to investigate it.

I am talking about the communication that Rabbi Hier has, not even necessarily the bomb response. But I think that a threat of that nature would be a sufficient predication for the FBI to open at least a preliminary inquiry.

Senator SPECTER. Well, Mr. Litt, let's move to another subject. The testimony that you provided says, quote, "The development of secure anonymous electronic mail will greatly impair the ability of law enforcement to track terrorist communications."

We know that after the Oklahoma City bombing, a number of anonymous bombmaking instructions were posted on the Internet. Where you have had traditionally anonymous communications, they are principally in the context of a one person to one person.

Do you see any problem beyond the one you articulated in having widespread anonymity among Internet users? And if so, is there anything that can be done about that?

Mr. LITT. I am not sure what you mean by the problem I articulated.

We perceive a serious danger to law enforcement, and let me, if I could, just play off of the example that Rabbi Hier just read there.

It is frequently, under existing circumstances, difficult or impossible to trace back who actually sent that message across the Internet. It may go through many different computers. They have what they call anonymous remailers, and some of the Oklahoma City postings that you referred to earlier were sent through anonymous remailers, the sole purpose of which is to make it difficult or impossible to trace back and identify these senders of the message.

This is an issue of extreme concern to law enforcement. There are social and technical advantages to anonymity, as well. I think, if you think about it in the context of whistleblowers or rape crisis groups, or so on, a similar issue is presented with respect to the matter of caller ID on telephones.

In my remarks, I suggest that the approach that we believe is appropriate is one of confidentiality, which allows individuals to remain anonymous but gives Government, the authorities, the right in appropriate circumstances to go behind that anonymity and ascertain who the sender of the message is.

Senator SPECTER. Mr. Burrington, the factor of anonymity is obviously an inherent factor in Internet. That is a part of the issue which has to be dealt with, is that correct?

Mr. BURRINGTON. I am sorry, Senator, I didn't——

Senator SPECTER. Is there no way to avoid anonymous messages through Internet?

Mr. BURRINGTON. Yes. I mean, not everybody is anonymous. I am going to let Jerry do the Internet part of this, but let me talk about the AOL, the America Online, or the online service perspective, because it is different, again.

We do allow people, in effect, to have screen names. The individual in this case, in this message, is "toughguypa," the one that we have been talking about here.

Obviously, maybe "nutguy" would be a better screen name for him.

But then, if we were required to—and this happens fairly frequently—the FBI could subpoena us and we could then go into that person's account and provide the FBI with that account information, just the basic information, name and address.

You know, when you talk about anonymity, there is anonymity, that is a feature of our service. We market it, actually, in terms of the sense that you can be who you want to be.

You, Senator Specter, could be a Democrat online and no one—if you wanted to be. [Laughter.]

There is an attractiveness to that because it draws out an opportunity to communicate in ways that people have never had before. But in the end, the buck ultimately stops somewhere, which is that we do know the identity of that person because we have to bill them. We know their address, you know, that kind of information.

That is the case of the closed, commercial, online service.

Senator SPECTER. But there are ways to use the system through a variety of devices so that that person, identifiable under some limited circumstances, then becomes anonymous.

Mr. BURRINGTON. Can I ask Mr. Berman to——

Senator SPECTER. Go ahead, Mr. Berman.

Mr. BERMAN. I think this is a fundamental issue. It is one of the issues that we would like to address in a study that Senator Leahy has proposed.

Because in talking about where is liability or where is responsibility in this new information highway, we have on the one hand the America Online, which is in the position of not being able to know what messages are coming across their net or their gateway to the Internet, but if we want to focus responsibility at the sender and recipient of messages, we have to, at some point, find a balance between anonymity and what the Justice Department calls confidentiality.

There is, I think, going to be growing pressure to have some kind of address book like the phone book on the information highway as part of doing business. It is one thing to have an unlisted number, but whether you can have a total anonymity and be able to send any kind of message across the net, I think that has to be addressed.

I think that there will be pressure on American onlines not to gateway and carry anonymous messages.

Senator SPECTER. What is your view of that, Mr. Berman? Should the gateway permit anonymous messages?

Mr. BERMAN. In order to balance all of the interests and that includes privacy—there is a right to anonymity, the Supreme Court just decided that there is, and we agree with that—but it can be abused, and I think that we are prepared to work, we don't know quite how to do it, yet, but to work on some sort of standard, whether it is voluntary or net-wide, which creates a presumption that there is some addressing.

Senator SPECTER. All right, gentlemen. Thank you very much. We are going to pursue some of the open-ended questions from today's hearings, specifically an analysis of what information is available.

Mr. Litt is going to provide it to us, to the extent he can, about manuals actually being inciting factors to the making of bombs which are used for criminal or violent purposes.

We will be watching the anonymity issue, and there is also the question as to obscenity going over Internet, which will be a major issue in terms of legislation which is already pending.

We thank you very much for joining us today, and that concludes our hearing.

CHORUS OF VOICES. Thank you, Mr. Chairman.

[Whereupon, at 11:22 a.m., the subcommittee was adjourned.]

APPENDIX

Questions and Answers

Responses of Mr. Litt to Questions Submitted by Senator Specter

Question 1. A recent New York Times article notes that the U.S. Government makes available to the public field manuals with titles like "Unconventional Warfare Devices and Techniques," "Boobytraps," "Improvised Munitions Handbook," and "Incendiaries." Many of these manuals end up in survivalist bookstores, and could easily end up online. How would you balance our concerns about these manuals being misused with the fundamental value we place on having an open government, whose work and products are available to the public through the Freedom of Information Act?

Answer. Balancing the public's right or need to know information against legitimate concerns regarding the distribution of information about explosives and other highly-destructive weapons is difficult. For example, a number of people, including the police, scientists, and engineering students, have a legitimate need to know how explosives work. Similarly, the public has a need to know under what conditions a commonly-available substance—such as gasoline or fertilizer—may explode. But, as you note, government manuals providing this information can be subject to catastrophic misuse.

Because the question relates to the appropriate amount of dissemination of information by the government, as opposed to restricting the distribution of information by private parties, the balancing of these interests is more a matter of policy than of constitutional law. Once information is appropriately released, law enforcement's goal is to ensure that the misuse of government information is deterred and punished. Law enforcement must be properly equippped to detect, investigate and prosecute such misuse. Mr. Litt's testimony on May 11, 1995, dealt at length with this issue.

Question 2. Is the constitutional right to assemble any different when it is on a computer chat area rather than in an assembly hall?

Answer. The law in this area is still unclear. Many computer "chat" areas, or other areas for public message posting on computer bulleting boards or networks, are run by private entities who are (for the most part) free under the First Amendment to restrict the use, of their facilities. But if the First Amendment does apply—for example, because a network is government-owned—the courts have not yet addressed how to treat an area on that network dedicated to public discussion, specifically, whether that area is some type of public forum. Assuming it is a public forum, the government could still enforce reasonable time, place and manner restrictions. Moreover, the government is free to enforce generally applicable laws, such as the threat and conspiracy statutes, in a public forum. On the other hand, if the forum is nonpublic, reasonable restrictions on speech are permissible if they are not a content-based effort to suppress speech.

At this point, however, the extent of reasonable regulation of speech in "cyberspace" is unclear, and may depend on the specific factual setting.[1]

Question 3. Last year, Carnegie Mellon University announced that it was eliminating from its computer network access to Internet discussion groups on sexuality because it did not want underage users of the system to have access to the sexually explicit material in those discussion groups. The school's computer services adminis-

[1] See generally David J. Goldstone, *The Public Forum Doctrine in the Age of the Information Superhighway (Where Are the Public Forums on the Information Superhighway?),* 46 Hastings L.J. 335, 350–357 (1995); Edward M. Naughton, Note, *Is Cyberspace a Public Forum? Computer Bulleting Boards, Free Speech, and State Action,* 81 Geo. L.J. 409, 424–28 (1992).

trator was fearful that the school could be held liable as a purveyor of pornography. Other schools with online discussion groups on their computer networks have similar concerns. Do schools have legitimate concerns over liability under current obscenity statutes for permitting sex discussion groups on their computer networks or for providing access to Internet sex discussion groups?

Answer. Under current law, any person who knowingly distributes obscenity in interstate commerce, or aids and abets others in such activity, may be subject to criminal prosecution; it is of course no defense that the person works for an educational institution. But to the extent obscene materials are posted without school personnel's knowledge or consent, those personnel need not fear prosecution under current law. We should note, however, that knowledge may be proved several different ways in the context of obscenity, including proof of willful blindness.

Question 4. The Supreme Court has justified less First Amendment protection for broadcast media than for print because of spectrum scarcity and because broadcast is viewed as intruding directly into the home through the TV or radio, unlike print which must be obtained outside the home or by mail. Has the Supreme Court addressed squarely the question of whether electronic communications over computer networks are like print and deserving of full First Amendment protection, or like broadcast, with some government regulation of content allowed?

Answer. The Supreme Court has not addressed squarely whether, for First Amendment purposes, electronic communications over computer networks are more similar to print or broadcast communications. However, the Court has declined to apply the less rigorous "broadcast" First Amendment standard to cable television operators, because cable television does not suffer from the same scarcity of channels for transmission.[2] Computer networks similarly permit a large number of speakers to communicate over a nearly infinite number of channels. And although intrusion into the home—the "uniquely pervasive" aspect of broadcasing—is possible through computer networks, this does not necessarily justify regulation of solicited electronic communications over computer networks.[3]

It should be noted that the phrasing of the question itself—are electronic communications over computer networks "like print . . . or like broadcast"—suggests that the new electronic environment can be neatly equated with some existing communications paradigm. In fact, the reason it is so difficult to establish meaningful, workable rules for computer networks is that they are not exactly like anything that has come before. Computer networks are, in some ways, like "common carriers" such as telephone companies; that is, individuals can use network facilities to communicate privately, and the networks do not censor those communications. But those networks are also similar to "broadcasters" in that networks allow messages to be distributed broadly without prior request or approval of the recipient, and they allow for the distribution of text and pictures, by subscription, much like a newspaper. Thus, in considering network regulation we must keep in mind the diverse nature of new technologies. "Each medium of expression . . . must be assessed for First Amendment purposes by standards suited to it, for each may present its own problems." *Southeastern Promotions, Ltd.* v. *Conrad,* 420 U.S. 546, 557 (1975).

Question 5. Is there any justification for regulating the content of electronic communications transmitted by computer more than we do paper communications in the form of books, magazines and pamphlets?

Answer. As we noted in response to the prior question, electronic communications are different from print media. The wide diversity of forms of communication over computer networks confounds any attempt to generalize about the extent of appropriate regulation of the content of all electronic communications. Writings, pictures, and voice, stored and interactive, all travel across networks. Some of these electronic communications are similar to reading a book, while others are closer to conversing on the telephone. Depending on the specific facts, regulation may be more or less appropriate, and the constitutional analysis may be different. For example, there might be reason to regulate the electronic transmission of contraband not protected by the First Amendment, such as stolen credit card numbers, more closely than "print" contraband, because of the ease of transmission inherent in the medium.

Question 6. There are efforts underway in Congress to regulate the content of online communications that are obscene and to extend that regulation to protected in-

---

[2] *Turner Broadcasting System, Inc.* v. *FCC,* 114 S. Ct. 2445, 2457 (1994).

[3] See *Sable Communications of California, Inc.* v. *FCC,* 492 U.S. 115, 128 (1989) (intrusion rationale does not apply to voluntary telephone calls). If, however, an electronic communication is unsolicited, then the "intrusion" rationale might apply. See *i.d., at 127–28; see also Rowan* v. *United States Post Office Dep't,* 397 U.S. 728 (1970) (upholding regulation of the sending of sexually explicit material through the mail).

decent communications. The legitimate concern prompting these legislative efforts is that children are able to get access to inappropriate, sexually explicit material on the Internet. What technological means, if any, are available for parents to control the access their children have to information that may be obscene or dangerous on computer networks?

Answer. Technological means exist, or are being developed, for parents to control their children's access to obscene or dangerous information available on computer networks. Software can for example, block access to Internet sites known to contain sexually explicit material. This protection is not perfect because such material may be concealed, the proliferation of on-line information sources renders such software protections quickly obsolete, and children can often gain access to the Internet through computers at school or at friends' houses. Of course, restrictions on access by children to print media are also incomplete.

Still, a parent can reduce the risks of his or her child accessing inappropriate materials. Parents can best reduce the risks by becoming involved in the computer activities of their children—looking at the services to which the children subscribe, setting reasonable rules and guidelines for computer use, and staying in touch with what the children are doing online.

Question 7. Administration witnesses at recent hearings have focused attention on the problem of criminals using encryption to scramble their communications over the telephone or on the Internet to avoid law enforcement surveillance. The Administration has implemented a key escrow scheme often called Clipper Chip, to address the encryption problem. One perceived flaw in the Clipper Chip scheme is that U.S. Government agencies hold the decoding keys to communications encrypted with Clipper Chip. What steps, if any, is the Administration or private industry taking to address that flaw? What suggestions do you have about finding a solution to address the encryption problem?

Answer. The Administration has had informal discussions with representatives of various segments of the business community regarding their possible interest in serving as Escrowed Encryption Standard key escrow agents. In general, the response has been one of uncertainty regarding the nature of the attendant duties, the liability risks, and the compensation prospects. Of late, however, several private enterprises have begun to show some interest in encryption escrowing systems. Several firms now appear interested in developing and making available to the public their own hardware-based systems that involve some form of key escrowing. At least one firm also has been developing a system intended to permit an effective key access system for encrypted software. As the Administration understands these various systems, all would require government agencies, or private parties lawfully entitled to acquire the plaintext of the information, to seek access to the necessary keys from one or more trusted keyholders. We believe that such systems could strike the appropriate balance between the needs of law enforcement and individual privacy.

We are pleased at industry's growing recognition of the need to combine strong cryptography with a suitable method of government access to communications and stored date,[4] when such access is needed and lawfully authorized to protect the interests of society. These issues are complex, and require further study.

Question 8. Some have expressed concern that threatening a member of the community via a telephone is prohibited while doing the same act over the Internet is not. Would the law set forth in 18 U.S.C. §876(c), which makes it a felony to transmit any communication containing any threat to injure another person, cover communications over the Internet?

Answer. Title 18, section 875(c) (not section 876, which applies to the mails), concerning the transmission of threats in interstate commerce, applies in full force to interstate communications over the Internet. In most cases prosecuted under section 875(c), the transmission in interstate commerce has been by way of an interstate telephone call. See, e.g., *United States* v. *Cox,* 957 F.2d 264, 265 (6th Cir. 1992) (telephone call from Indiana to Kentucky). In other cases, however, the interstate nexus was another facility. For example, in *United States* v. *Kelner,* 534 F.2d 1020 (2d Cir.), cert. denied, 429 U.S. 1022 (1976), the threats were made before television news cameras, and subsequently were broadcast on a television news program.

[4] Encryption poses difficulties for law enforcement not only with respect to communications, but also stored data. A few years ago encryption of data was unknown; now, the FBI's Computer Analysis and Response Team reports that it encounters encrypted files in two percent of searches. We expect this number to grow exponentially as software vendors incorporate encryption into their commercial products. In fact, one commercial vendor recently has announced the availability of a sophisticated encryption program that will run under several major microcomputer operating systems.

Thus, section 875(c) is not limited to the telephone, but applies to any interstate transmission.

Question 9. The Department of Justice has characterized as "a critical issue" the use of anonymous electronic mail, which can impair the ability of law enforcement to track criminal electronic communications. How do anonymous remailers work and what records, if any, do the administrators of such services maintain on the electronic communications they remail?

Answer. Anonymous remailers accept electronic mail messages, strip them of identifying information, and forward them to the intended recipients. Messages are remailed in a random order to make tracing by matching incoming with outgoing messages more difficult.[5] The records kept vary from device to device. For example, some remailers assign an identification number to users, of which the system administrator keeps a list.[6] Other remailers could keep different records, encrypted records, or no records at all.

Thus, anonymous remailers—particularly if they keep a few or encrypted records—can present difficulties when law enforcement attempts to trace an electronic mail message. To be sure, anonymity can also be achieved with anonymous telephone calls or unsigned regular U.S. Mail, but because electronic mail is extremely inexpensive and can be sent to many people (rather than to a few or one) with little or no increase in cost, it poses unique problems to law enforcement (and civil plaintiffs, for example, in the case of "computer" defamation). In addition, regular mail and telephone calls will normally leave physical or electronic clues that are difficult and expensive to destroy completely, whereas electronic mail sent through a sufficiently sophisticated anonymous remailer can easily be made nearly untraceable.[7]

Question. 10. The Supreme Court in *McIntyre* v. *Ohio Elections Comm'n,* slip op, No. 93–896 (April 19, 1995), recently ruled that the First Amendment protects the freedom to publish political and literary speech anonymously. As the Court pointed out, "Anonymity is a shield from the tyranny of the majority." Id. at 23. What restrictions, if any, on anonymous electronic mail would pass constitutional muster under *McIntyre*?

Answer. As both the majority and the concurring opinions acknowledged, the ultimate scope of *McIntyre* v. *Ohio Elections Comm'n,* 115 S. Ct. 1511 (1995), is not settled. *See* 115 S. Ct. at 1522; id. at 1524 (Ginsburg, J., concurring). *McIntyre* clearly indicates a strong preference for dealing with illegal or tortious speech through post hoc remedies such as defamation suits or criminal charges, rather than by prophylactic requirements of public disclosure. But the Court has condoned other laws which either restrict anonymity directly or have that effect.[8]

Society must draw an appropriate balance between the indisputable need for anonymity in many contexts, such as when individuals have a legitimate need to avoid embarrassment or harassment, and the public interest in accountability. *McIntyre* did not resolve how to balance these interests for electronic communications, especially given the unique considerations that apply to anonymity on computer networks.[9] And *McIntyre* should not prohibit less intrusive (and narrowly-tailored) reg-

---

[5] See Peter H. Lewis, *Computer Jokes and Threats Ignite Debate on Anonymity,* N.Y. Times, December 31, 1994, at 1 & 53.

[6] See Lewis, supra; George P. Long, III, Comment, *Who are You?: Identity and Anonymity in Cyberspace,* 55 U. Pitt. L. Rev. 1177, 1184 (1994).

[7] See I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace",* 55 U. Pitt. L. Rev. 993, 1010–1012 (1994).

Similarly, some companies are now beginning to offer telephone customers the ability to place calls anonymously. The customer dials a "900" number that permits him to then dial another number via that service (similar to an anonymous remailer). The customer's long distance carrier, therefore, only has a record of the call to the "900" number, and has no record of the final destination of the long distance call. See Sue Reinert, *Without a Trace; For a Premium Phone Calls can Remain a Secret,* The Patriot Ledger, February 15, 1992.

[8] See *Riley* v. *National Federation of the Blind of North Carolina,* 487 U.S. 781, 795, 800 (1988) (noting in dicta that the State could constitutionally require a fundraiser to file detailed financial disclosure forms, which the State could publish); *Buckley* v. *Valeo,* 424 U.S. 1, 75–76 (1978) (permitting some disclosure requirements for those engaging in contributing to elections); *Whalen* v. *Roe,* 429 U.S. 589 (1977) (upholding a law that required state officials to record information regarding frequently abused prescription drugs); *United States* v. *Hariss,* 347 U.S. 612 (1974) (lobbyists). See also *Ryan* v. *County of DuPage,* 45 F.3d 1090, 1095 (7th Cir. 1995) (finding no constitutional right to wear a mask in a courthouse).

[9] Anonymity on the Internet poses greater problems than anonymity in other contexts. As discussed in the response to the prior question, electronic mail is extremely inexpensive, can be sent to numerous parties with little or no increase in cost, and can be made nearly untraceable. Thus, for example, anonymous mass distribution of illegally copied software poses a considerable risk to copyright holders. Prevention of widespread crimes involving information or possible

ulation of anonymity through, perhaps, requiring electronic communications services, including anonymous remailers, to keep records regarding the identity of their users, without the sort of public identification requirement invalidated in *McIntyre*. Because of the competing public and private interests involved, and the changing technology, we urge Congress to move carefully in this area.

---

speech, such as copyright infringement, defamation, and anonymous threats, constitutes a substantial state interest.

ADDITIONAL SUBMISSIONS FOR THE RECORD

LETTER FROM SENATOR KENNEDY REGARDING FIRST AMENDMENT PROTECTIONS AND TERRORIST MATERIALS ON THE INTERNET

April 28, 1995.

DEAR FRIEND: Thank you for contacting me about the issue of terrorism and the Internet. The issue is a very important one, and I welcome the fact that in response to my comments at yesterday's hearing by the Senate Judiciary Committee, so many people from different parts of the country have used e-mail to contact me on both sides of the issue.

As you know, I am a strong supporter of the Internet and the vast potential of the technological revolution to improve communication in our society and provide extraordinary access to information for large numbers of our citizens.

Our country is rapidly entering this new information age. Through computer networks, Americans enjoy increased access to a wide range of information, including government documents, educational resources and the views of their fellow citizens. The free flow of information on these networks is essential. But I am concerned, as I believe many citizens are, by the apparently easy access via the Internet to information whose only purpose seems to be to incite violence and terrorism.

We have only just begun to consider these complex issues in Congress, and clearly we must do so with the full regard for freedom of speech and other basic liberties protected by the Constitution.

As I have stated many times in the Congressional debate on pornography on the Internet, we must exercise the utmost caution if we are to legislate in this area. The constitutional right of free speech clearly applies to electronic communications, just as it applies to written or spoken communications.

For example, while the government can constitutionally limit material that falls within the narrow definition of obscenity, proposals that would impose excessive restrictions, such as the pending Exon Amendment, are too sweeping to pass constitutional muster.

Similar constitutional standards apply to terrorist materials on the Internet. While most speech is protected, no matter how unpopular, no one has a constitutional right to shout "fire" in a crowded theater, to threaten others with violence, to incite a riot, or to incite an act of terrorism. Similar constitutional principles allow Congress to prohibit the publication of military secrets.

In a recent example, Congress enacted in 1994 a law to protect women's health clinics from bombings and other violence. This bipartisan statute, which includes restrictions on protesters near the clinics, was crafted after a thorough examination of constitutional rights, and has been repeatedly upheld by federal courts.

Clearly, when Congress does act, it has a responsibility to do so in full accord with the Constitution and its fundamental protections for freedom of speech.

Thank you again for contacting me on this important subject. I will certainly keep your views in mind as Congress considers this critical issue in the coming weeks.

Sincerely,

EDWARD M. KENNEDY,
United States Senator.

PREPARED STATEMENT OF PEOPLE FOR THE AMERICAN WAY ACTION FUND SUBMITTED BY LESLIE HARRIS AND JILL LESSER

People For the American Way Action Fund (the "Action Fund") submits this testimony to emphasize the importance of the First Amendment in discussions concerning government control of speech on the Internet and other online networks. The Action Fund is a 300,000 member organization committed to preserving the central values of the First Amendment by promoting tolerance, free expression and vigorous public debate. We applaud Chairman Arlen Specter and the Judiciary Committee for holding this hearing on these issues of critical importance in the information age.

The American political landscape for years has been populated with people who spread reckless and violent rhetoric. Such rhetoric and the debate that it has spurred in the aftermath of Oklahoma City is particularly troubling to The Action Fund, which is committed both to protecting freedom of expression and to promoting a climate of tolerance and community. We believe that when presented with difficult issues like how we should respond to political figures who tell supporters that their

opponents are out to destroy American society or to broadcasters who tell their listeners or viewers that the government is the enemy of the people, feeding fears that this nation's family, faith and freedoms are under imminent threat of destruction, the answer is not to silence such speech but to encourage more speech in response.

We are at the same time very concerned about the existence of "hate speech" and are unwilling simply to join the chorus of people who claim that such speech has absolutely no impact on behavior. We believe very strongly that ideas do indeed have consequences. We do not believe that the existence of such consequences, however, makes the case for government censorship. Instead, we must respond to intolerant and violent rhetoric by encouraging Americans to stand against those voices and emphasize the American values of liberty, justice and respect for the differences inherent in a vibrantly pluralistic society. The "marketplace of ideas" strengthens democracy when everyone takes the responsibility to be engaged in the debate. We advocate not censorship, but citizenship.

In the wake of the horrible bombing in Oklahoma City, citizens of this nation are rightly concerned with activities that appear to threaten the safety of American citizens. But the Action Fund believes that we must not let that incident diminish this nation's commitment to the First Amendment. Policy makers should not use this tragic incident to undermine the positive unifying aspects of speech on computer networks and the value those networks add to society. The Internet and other online computer networks are already transforming the way people in this country and around the world communicate, entertain themselves and behave as political creatures. The fact that these new technologies offer powerful modes of information dissemination cannot alone justify government intervention and intrusion into the constitutional rights of American citizens. If we do so, the value of such networks will diminish, leaving this nation's role in the information age and the values of the First Amendment threatened.

The Action Fund acknowledges that the specific intent of this hearing is to address the narrow questions raised by the government's power to investigate and infiltrate the purveyors of violent or mayhem-inducing computer communications. And, we agree with the general conclusion of the testimony being presented at this hearing by Jerry Berman of the Center for Democracy & Technology that the federal government already has ample investigative and surveillance tools to ensure adequate protection of the American public from violent speech on the Internet.

However, we are submitting our own testimony because we also feel strongly that the question of whether the government should control, track or investigate violent speech in the new online environment is only one among many dilemmas that have surfaced in response to the proliferation of computer networks and their apparent ubiquity. For example, just in the first three months of the 104th Congress, we have seen significant attention paid to legislative proposals that seek to restrict the transmission of sex-related or adult material on the significant attention paid to legislative proposals that seek to restrict the transmission of sex-related or adult material on the same computer networks.

While the legal analyses may differ slightly in particular circumstances, the Action Fund believes that it is inadequate to address government response to violent speech in the online environment without recognizing that content regulation in one subject area sets precedents for content regulation on other areas. This Committee must scrutinize very carefully any efforts to restrict or monitor any category of speech online which could not lawfully be restricted or investigated in a bookstore, library, newsstand, town square or other context.

The Internet and other computer networks are unique. They enable Americans to become publishers of information with the stroke of a key. In that way such networks operate like distributors of newspapers or pamphlets put out by individual citizens. Resources like the World Wide Web greatly expand the sources of information available to individuals in their own homes and enlarge the impact that any one citizen with relatively few resources can have on public debate.

The inherent potency of these networks in shaping debate must not be used to justify government monitoring and censorship. Instead, it should be seen as an opportunity to enhance democracy—to encourage more Americans to use these technologies to respond to rhetoric they find either helpful or abhorrent. While the tragedy in Oklahoma has made many in this country question the implications of unfettered speech in several arenas, most specifically in the media, it is important to remember that speech in this country often serves its highest value when it challenges our beliefs and values. It is a basic tenet if American society that effective discourse emerges most readily out of heated emotions, be they positive or negative. And it is through effective discourse that conflicts are often peaceably solved.

One of the most disturbing elements of the recent attempts to censor speech on the Internet and other computer networks is the general lack of familiarity with the

technology and the resulting willingness by policy makers to enact restrictions of speech, rather than explore the ability of the technology itself to empower users to make decisions about the kinds of content to which they have access. The debate during this Congress has largely centered on the Communications Decency Act (S. 314), introduced by Senators Exon and Gorton, and recently added to the S. 652, the pending telecommunications reform legislation. That legislation would establish an outright ban on speech that is indecent, lewd, lascivious or filthy but nonetheless fully protected by the Constitution, without any examination of the legislation's First Amendment implications or the technological tools that may be available to enable adult users to make personal content decisions.

The Action Fund urges this Committee to recognize that the Internet and other computer networks hold vast possibilities for the reinvigoration of democratic discourse in this country. Neither the unfamiliarity with the technology, nor the fear invoked by recent acts of random violence or the worry about access by our nation's children to adult-oriented materials, should lead Congress irreparably to damage the usefulness and importance of those networks without a complete examination of both the constitutional implications of restricting certain speech and all facets of the technology.

○

36-038 (76)

ISBN 0-16-053965-X
90000
9 780160 539657